Uno scorcio di un ufficio virtuale del Web, realizzato in VRML.

Telefonare tramite la Rete

Se avete un computer adeguatamente attrezzato con una scheda audio, un microfono e degli altoparlanti, Internet vi consente di fare telefonate internazionali o intercontinentali al costo di una telefonata urbana.

C'è una folta schiera di programmi per telefonare attraverso Internet. Il programma chiamato *Internet Phone*, prodotto dalla VocalTec (http://www.vocaltec.com) è stato il capostipite di questo tipo di programmi per gli utenti di personal computer e ha dato il nome all'intera categoria.

Gli Internet Phone sono stati trattati inizialmente dai media come poco più che una stravaganza, e le società telefoniche li hanno snobbati, dicendo che si trattava di una meteora destinata a spegnersi ben presto e che non destava preoccupazioni di concorrenza.

Ora cominciano a preoccuparsi seriamente, tanto che Deutsche Telekom (la Telecom tedesca) ha da tempo acquistato una quota della VocalTec: se non puoi batterli, unisciti a loro, insomma. Telecom Italia prevede di perdere l'8,3% del proprio traffico internazionale, pari a circa 270 miliardi, a causa degli Internet Phone entro il 2001.

Come funziona

Quando parlo di "telefonare" attraverso Internet, non mi riferisco alla digitazione di messaggi: intendo dire proprio l'atto di parlarsi come al telefono, in modo interattivo, facendo sentire all'interlocutore la propria voce reale. Ma come diavolo è possibile?

I programmi come Internet Phone si basano su una cosa chiamata *compressione audio digitale*. In pratica, quando usate Internet Phone, non fate altro che parlare in un microfono collegato ad una comune scheda audio installata sul vostro computer.

Il computer, tramite il programma Internet Phone, trasforma la vostra voce in impulsi digitali che trasmette attraverso la Rete (come se si trattasse di un qualsiasi file o documento) al vostro interlocutore. Una volta arrivati a destinazione, gli impulsi vengono riconvertiti in suoni e trasmessi agli altoparlanti collegati all'apparecchio del destinatario.

Se avete un minimo di dimestichezza con la registrazione di suoni tramite il computer, saprete che normalmente una registrazione audio occupa una quantità di spazio spropositata. Trasmettere un normale file contenente una registrazione audio richiederebbe un tempo lunghissimo e quindi una conversazione a ritmi normali (botta e risposta) sarebbe impossibile.

È qui che entra in gioco la compressione: si può "compattare" una registrazione audio per farle occupare meno spazio, ad esempio sostituendo le pause con la breve istruzione "pausa di un decimo di secondo". Internet Phone e soci eseguono questa compressione automaticamente e "al volo", cioè mentre state ancora parlando, e usando particolari sistemi studiati appositamente per la telefonia. La quantità di dati da trasmettere viene così ridotta in modo impressionante, rendendo praticamente istantanea la trasmissione della registrazione digitale della vostra voce.

L'Internet Phone del vostro interlocutore, a sua volta, scompatta la registrazione digitale altrettanto "al volo", cioè mentre la sta ancora ricevendo, e la passa alla scheda audio del computer per suonarla attraverso gli altoparlanti.

Incredibile a dirsi, l'intero procedimento è in genere talmente veloce che si ha la stessa sensazione di ritardo che si avverte durante le normali conversazioni intercontinentali. Le vostre parole giungono alle orecchie del vostro interlocutore circa un secondo dopo che le avete pronunciate, per cui diventa possibile parlarsi come se si fosse al telefono.

Il potere rivoluzionario della tecnologia di Internet Phone sta proprio nel fatto che si ha una vera e propria conversazione: un'interazione diretta in cui sentite la viva voce dell'altra persona, con tutte le sue inflessioni emotive, le pause e le esclamazioni. Più di ogni altro servizio Internet, questo è quello che vi dà la vivida sensazione che dietro ogni schermo di Internet c'è una persona reale.

Quanto costa e cosa occorre

Usare un Internet Phone ha soltanto tre fattori di costo:

- l'hardware (scheda audio, microfono e una cuffia o degli altoparlanti, se non li avete già)
- il programma
- la telefonata fino al vostro fornitore d'accesso.

La prima voce è quella più costosa: ci vuole una buona scheda audio: possibilmente del tipo *full duplex*, in modo da poter parlare e ascoltare contemporaneamente, altrimenti sarete costretti a parlare a turno, come i radioamatori. Il microfono, invece, può costare anche solo ventimila lire: non è importante la qualità, basta che funzioni.

La spesa per il programma è la meno dolorosa: infatti la maggior parte degli Internet Phone è distribuita gratuitamente ed è liberamente prelevabile dalla Rete. In alcuni casi potete prelevare soltanto una versione dimostrativa, nella quale le conversazioni possono durare un minuto e mezzo all'incirca. In genere, comunque, se c'è qualcosa da pagare, si tratta di circa centomila lire, che si ripagano facilmente con il risparmio in bolletta.

Una volta pagato il programma, il mondo è vostro al costo di una telefonata urbana. Infatti soltanto le due tratte iniziali e terminali della conversazione avvengono sulla normale rete telefonica. Il resto passa via Internet.

Questo significa che voi pagate la telefonata urbana per collegarvi via modem al vostro fornitore d'accesso, e il vostro interlocutore fa altrettanto per collegarsi al suo. La tratta rimanente, non importa quanto sia lunga, è gentilmente offerta da Internet.

Giusto per chiarire ancora meglio i termini della questione, facciamo un esempio pratico. Io sto a Pavia e voglio comunicare con un parente che sta in Australia. Mi collego a Internet tramite il mio fornitore d'accesso nella stessa città e pago quindi la tariffa Telecom urbana, poi avvio il mio Internet Phone.

Contemporaneamente, il mio parente (chiamiamolo Ugo, per comodità) fa la stessa cosa a casa sua a Melbourne; anche lui paga la sua eventuale tariffa urbana (in molti paesi, come gli Stati Uniti, le chiamate urbane non si pagano).

Il costo di questa telefonata intercontinentale è dato dalla somma della mia tariffa urbana Telecom e della (eventuale) tariffa urbana di mio zio Ugo. Spannometricamente, significa spendere al massimo cinquemila lire l'ora contro la tariffa Telecom di tremila lire al minuto. Devo aggiungere altro?

Difetti

E allora perché non abbiamo giù tutti mandato a quel paese Telecom Italia, Infostrada e compagnia bella e non ci siamo messi ad usare un Internet Phone?

Perché, come si dice su Internet, *TANSTAAFL* (la spiegazione di questa sigla è nel Glossario): il risparmio offerto dagli Internet Phone ha una contropartita. A parte la spesa iniziale, ci sono alcune limitazioni tecniche non trascurabili.

- Per prima cosa, non potete telefonare a chiunque via Internet: perlomeno non a questi prezzi stracciati. Potete parlare a tariffa urbana soltanto con le persone che hanno un account alla Rete e dispongono di un computer attrezzato adeguatamente (i terminali offerti da molte aziende e istituti universitari, i set top box e le console non vanno bene).
- C'è anche un altro inconveniente, ed è più serio: l'interlocutore deve essere *online*, cioè collegato a Internet, proprio nel momento in cui cercate di contattarlo, e deve aver attivato il suo Internet Phone, altrimenti non c'è niente da fare. È come telefonare a qualcuno che ha staccato il telefono dalla presa.
- Un ultimo fattore limitante è che il carico di dati prodotto dagli Internet Phone è molto intenso e molti siti stanno iniziando a rifiutare l'accesso agli utenti che vogliono comunicare a voce.

Ovviamente tutte queste limitazioni pratiche sono poco importanti se dovete comunicare sempre con la stessa persona o con lo stesso gruppo di persone: basta mettersi d'accordo.

Se durante la vostra vacanza in California avete conosciuto una ragazza di cui vi siete invaghiti, e lei ha ricambiato, potreste corrispondere via e-mail e concordare di darvi appuntamento con Internet Phone ad una certa ora di un certo giorno della settimana. Dovreste assicurarvi di aver trovato una californiana che conosce il surfing su Internet bene quanto quello sulle onde del Pacifico, e dovreste sapere benino l'inglese, ma questi sono dettagli che Internet Phone non può risolvere per voi.

Infine c'è un inconveniente occasionale ma non per questo meno fastidioso: gli attuali Internet Phone producono talvolta un suono gracchiante e metallico, spesso perdendo parti della conversazione; è un po' come ascoltare una radio lontana in onde medie.

Probabilmente le versioni successive di questi programmi miglioreranno le proprie prestazioni, ma se volete essere sicuri di sentire quello che vi sta dicendo il vostro interlocutore, per ora vi conviene usare il caro, vecchio telefono.

Servizio universale: Net2Phone

Dicevo prima che i normali Internet Phone vi consentono di comunicare soltanto con un altro utente

Internet e soltanto dopo aver concordato un orario nel quale vi collegherete entrambi alla Rete. Scomodo.

Entra in scena a questo punto un nuovo tipo di Internet Phone: un programma gratuito che vi permette di telefonare da Internet a chiunque abbia un comune telefono e oltretutto senza doversi dare appuntamento, come ad esempio *Net2Phone* (http://www.net2phone.com).

Certo, le chiamate non sono così a buon mercato come quelle degli Internet Phone normali, dato che da Internet al telefono del destinatario viaggiano sulla rete telefonica ordinaria, ma si spende decisamente poco: 180 lire al minuto per l'Inghilterra, 72 per gli Stati Uniti, 250 per raggiungere di giorno i costosissimi telefonini "family" o il resto d'Europa.

Funziona? Beh, io sono rimasto piacevolmente sorpreso. È importante avere un fornitore d'accesso Internet ben collegato al resto della Rete e conviene chiamare in orari di basso traffico, ma tutto sommato le prestazioni sono accettabili.

Se siete incuriositi, potete prelevare il programma e provarlo gratis conversando (se ve la cavate con l'inglese) con gli operatori del servizio Net2Phone.

Se siete convinti, comprate qualche minuto di traffico con la vostra carta di credito e poi stupite gli amici: quando vi chiederanno "Da dove chiami?" potrete rispondere "Da Internet!".

Ci vediamo su Internet?

Io sono uno di quegli utenti della "vecchia guardia" che ancora si meraviglia per la velocità dell'e-mail: per me un Internet Phone è quasi fantascienza. Eppure non è l'ultima parola in fatto di telecomunicazioni via Internet: esistono anche programmi che oltre alla voce vi fanno vedere il vostro interlocutore.

Uno di essi si chiama *CU-Seeme*, che è una storpiatura della frase inglese *"see you, see me"*, vale dire "io vedo te, tu vedi me". Il nome dice tutto del programma: è un videotelefono che funziona via Internet.

Se un Internet Phone ha dei costi d'avvio non trascurabili, programmi come CU-Seeme sono ancora più cari. Infatti occorre aggiungere a tutti i componenti che ho citato prima anche una telecamera digitale da collegare al vostro computer.

L'immagine è per ora ai limiti dell'accettabile: sgranata, a scatti e molto piccola, anche nei momenti migliori e con connessioni molto veloci. Tuttavia è un primo passo e man mano che la capacità di traffico di Internet aumenterà, la qualità di questi sistemi migliorerà di pari passo. Già ora, le reti di computer interne delle aziende, che collegano filiali distanti tramite connessioni ad alta velocità,

permettono di fare videoconferenza senza problemi.

Chiacchierare in diretta: Internet Relay Chat

L'e-mail è veloce, ma non vi permette di fare delle vere e proprie conversazioni a "botta e risposta". Per questo ci vuole un servizio chiamato *Internet Relay Chat*, abbreviato in *IRC*.

Con IRC, Internet offre la possibilità di "dialogare" in diretta con altri utenti situati in qualsiasi parte del mondo, facendo conversazione a due o in gruppo. Ognuno digita sul proprio computer quello che vuole dire e le sue parole vengono viste da tutti i partecipanti, in tempo reale o quasi, indipendentemente dalla distanza che li separa e sempre al costo di una telefonata locale. Se dovete tenere contatti con persone lontane, può essere una magnifica alternativa alle telefonate.

Ci sono due modi fondamentali di usare IRC. Uno è per le conversazioni "uno a uno"; l'altro è per le discussioni di gruppo. Nel primo caso IRC ha una funzione personale, pratica e vantaggiosa, perché vi consente di comunicare con persone che conoscete. Nel secondo diventa purtroppo un servizio ad alto tasso di frivolezza. Come nelle *chat line*, si passa infatti moltissimo tempo a dialogare con sconosciuti di cose irrilevanti e alla fine ci si stufa (va a gusti, ovviamente, ma io ho rinunciato dopo mezz'ora).

Negli ultimi tempi, il disinteresse verso tutto ciò che non sia multimediale, squillante e colorato nell'universo di Internet ha prodotto una nuova serie di alternative all'IRC, in cui non ci si limita a scambiare messaggi di testo ma si scambiano immagini o si opera in un ambiente tridimensionale in cui ogni partecipante assume un "corpo" virtuale, chiamato *avatar*, a sua scelta.

Qui vi descrivo principalmente l'IRC "tradizionale", visto che rimane il più diffuso.

Come funziona l'IRC

L'Internet Relay Chat si basa su un gran numero di siti dedicati, presso i quali sono a disposizione dei computer, chiamati *server IRC*, che ospitano le conversazioni. Ciascun server appartiene a una di circa trenta reti IRC che coprono il mondo. Ciascuna rete è suddivisa in *canali*, ognuno dedicato ad uno specifico argomento. Ci sono circa tremila canali differenti.

Potete paragonare ciascun canale di IRC a una stanza virtuale nella quale ci si riunisce per discutere intorno a un determinato tema. In realtà poi le discussioni partono da un argomento per divagare molto spesso, ma questa è un'altra storia.

Per interagire con l'IRC ci vuole un programma, chiamato tecnicamente *client IRC*, che vi permette di collegarvi a uno dei server IRC di una rete di Internet Relay Chat. Quello che scrivete collegandovi a un server di una rete viene diffuso quasi istantaneamente a tutti gli altri server della rete, ovunque siano nel mondo.

In questo modo chiunque sia collegato al vostro canale, da qualsiasi parte del globo, potrà leggere le vostre parole e rispondervi (quasi) istantaneamente.

Il programma di IRC vi permette in genere di creare canali "personali" o privati, decidere chi può parteciparvi e talvolta anche di scambiare file.

Programmi da usare

Come per gli altri servizi della Rete, su Internet trovate molti programmi gratuiti o shareware anche per l'IRC. Di gran lunga, però, il più usato è *mIRC* (http://www.mirc.com) per l'ambiente Windows; è shareware e semplifica notevolmente i rituali di collegamento. Chi ha un computer Mac può provare *Ircle* (http://www.ircle.com), e ci sono programmi per IRC adatti a qualsiasi tipo di apparecchio collegabile a Internet.

Configurare un client IRC, ossia immettere i parametri giusti per farlo funzionare, non è difficile; richiede solo un po' di pazienza. Vi descrivo qui brevemente quello che occorre fare per attivare il programma mIRC.

- **Dati personali.** Dovrete immettere il vostro nome e cognome, il vostro indirizzo di e-mail (eventualmente alterato per sicurezza) e il vostro *nickname* (*"nic-nèim"*), ossia lo pseudonimo con il quale volete farvi conoscere in Rete.
  Se volete restare relativamente anonimi, potete immettere un nome di fantasia. Consiglio alle Internettiste di non rivelare che sono donne: ci sono parecchi molestatori (verbali) nell'IRC.
  L'indirizzo di e-mail è "anonimizzabile" soltanto fino a un certo punto: la parte dopo la chiocciolina verrà comunque corretta dalla Rete in quella autentica, anche se la immettete fittizia.
  Tenete presente che questi dati verranno trasmessi a chiunque digiti i comando */whois*, che rivela eventuali informazioni personali che avete immesso.
- **Il server IRC**. Dovete specificare a quale server desiderate collegarvi: la scelta è vasta, ma conviene un server situato in Italia. La lista aggiornata (con cambiamenti frequentissimi) è facilmente reperibile in Rete immettendo in un motore di ricerca le parole *IRC servers* e *Italy* o *Italia*.

Queste sono le impostazioni di base: dovreste poter lasciare invariati tutti gli altri parametri. Giusto per completezza, vale la pena di notare che mIRC consente anche di scavalcare i server IRC e

intavolare una conversazione diretta, più riservata, con un interlocutore dotato dello stesso mIRC.

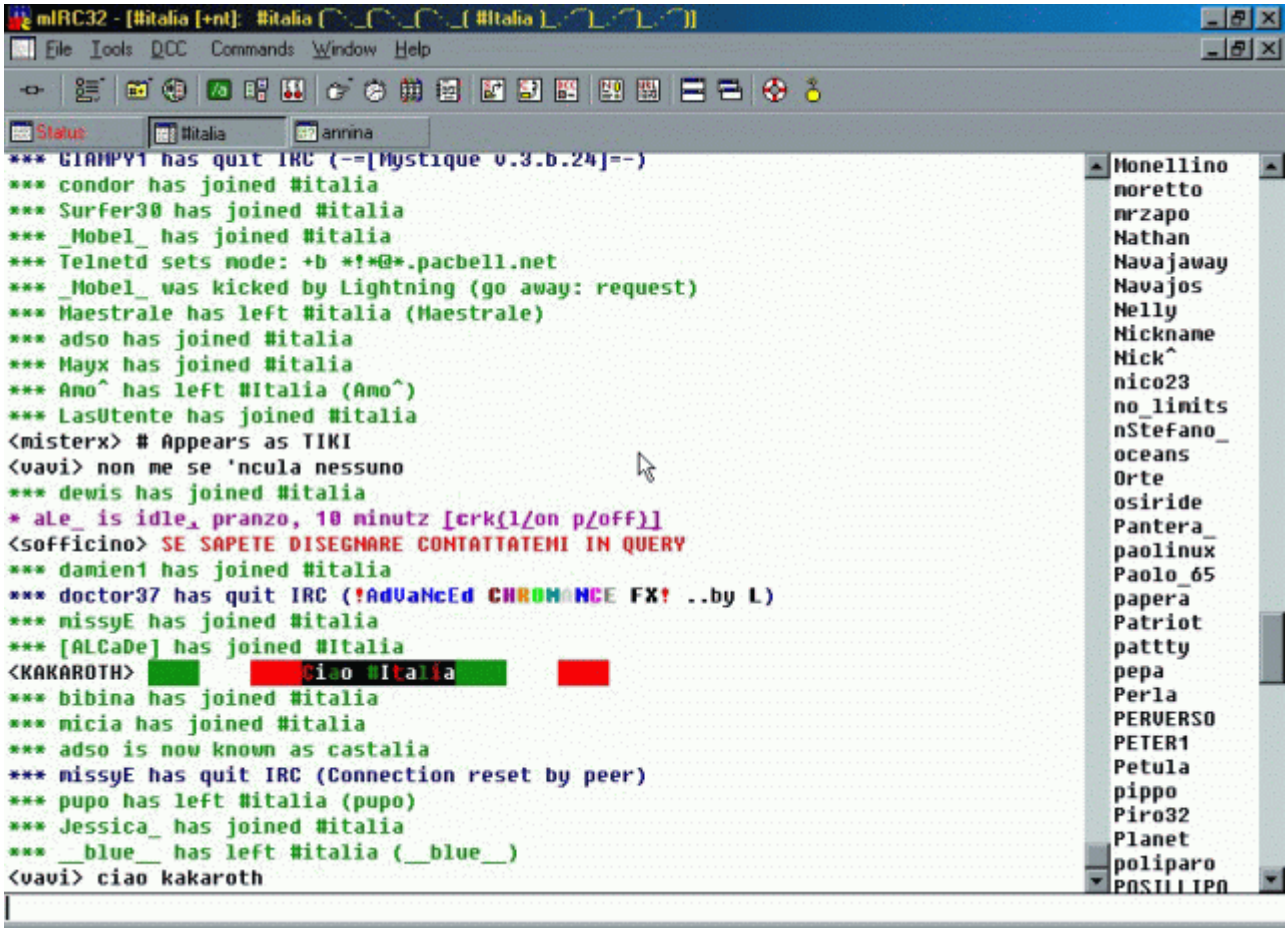
Per iniziare una sessione di IRC bisogna ovviamente essere prima collegati a Internet, come per gli altri servizi della Rete, e poi collegarsi al server IRC. Questo secondo collegamento può richiedere una certa attesa (diciamo un paio di minuti).

Una volta stabilito il collegamento IRC, comparirà un elenco di canali. Scegliete quello dedicato al tema che vi interessa e unitevi alla discussione con l'apposito comando del vostro programma (in mIRC è *Join*).

A questo punto comincerete a veder scorrere sullo schermo le parole degli altri partecipanti. Provate a scrivere qualcosa di blando, tipo *"salve"* e premete Invio. Questo serve a far sapere agli altri del vostro arrivo.

Vi conviene stare zitti per un po', come fareste prima di unirvi a una conversazione reale, per capire che aria tira. Ogni volta che qualcuno scrive qualcosa e preme Invio, compare una nuova riga di testo accanto alla quale c'è il nickname della persona che ha scritto il messaggio.

Per uscire da un canale che non vi interessa, in mIRC scegliete il pulsante *Close*.



Una sessione di IRC con mIRC, nel canale *#italia*. Immagine cortesemente fornita da Sergio Sanges (navajos@tin.it).

I comandi principali dell'IRC

La maggior parte dei comandi dell'IRC è gestita tramite pulsanti in programmi come mIRC, ma vi conviene comunque conoscerne la sintassi. Tutti i comandi dell'IRC iniziano con la barra (il simbolo "/"). Ecco i principali:

- **/join** #. Seguito da un nome di canale, vi collega a quel canale. Se il canale non esiste, questo comando ne crea uno nuovo.
- **/help**. Seguito dal nome di un comando, vi spiega il funzionamento di quel comando. Di solito lo fa in inglese, il che non sempre equivale a una spiegazione, ma tant'è.
- **/part** #. Seguito dal nome del canale, vi scollega dal canale stesso. Se non specificate il nome del canale, verrete scollegati dal canale nel quale siete in quel momento.
- **/quit**. Questo comando vi scollega completamente dal server IRC.

- **/list**. Elenca tutti i canali del server al quale siete collegati.
- **/who**. Elenca tutti i partecipanti al canale nel quale vi trovate.
- **/whois**. Seguito da un nickname, restituisce le informazioni pubbliche del proprietario di quel nickname (quelle che ha immesso nel proprio programma per IRC).
- **/nick**. Seguito da un nickname, sostituisce il vostro pseudonimo attuale con uno nuovo. Se il nickname è già utilizzato da qualcun altro, vi verrà chiesto di sceglierne uno diverso.
- **/ignore**. Seguito da un nickname, ignora tutti i messaggi provenienti da un utente specifico (quello indicato dal nickname). Se qualcuno vi scoccia, potete zittirlo con questo comando: non vedrete più i suoi messaggi.
- **/msg**. Seguito da un nickname, invia un messaggio riservato all'utente che ha quel nickname.
- **/motd**. Sta per *message of the day* ("messaggio del giorno") ed elenca le regole d'utilizzo del server.

I canali italiani di IRC

Se avete dimestichezza con i newsgroup, l'organizzazione dei canali di IRC non vi sembrerà complicata. Chiunque può aprire e chiudere un canale in qualsiasi momento, per cui quelli disponibili cambiano in continuazione. Molti, però, sono stabili e ricorrenti, soprattutto di sera.

Come per i newsgroup, anche per l'IRC esistono innumerevoli aree di discussione in italiano, ciascuna dedicata ad un tema specifico: ad esempio *#mp3.it* oppure *#mp3.ita* per lo scambio di musica digitale fra appassionati (violando sfacciatamente le norme sul diritto d'autore), *#icling* (dedicato a chi vuole esplorare le magagne dell'inglese dal punto di vista degli italiani), e i più "caldi" *#idsessualita*, *#idsentimenti* e *#isd.channel*.

Io ci sono, tu C6?

Ci sono navigatori che amano la solitudine e ci sono utenti che adorano la compagnia. Confesso di essere uno del primo gruppo: quando sono su Internet, di solito è perché ci sto lavorando e ho delle scadenze da rispettare e delle soluzioni precise da trovare; anche quando non ci lavoro, mi piace essere libero di concentrarmi su quello che sto leggendo o facendo con la Rete. Ho già due gemelle di due anni e mezzo che mi offrono interruzioni non previste in abbondanza, per cui difficilmente ne cerco di ulteriori.

Ma so che non tutti sono come me. C'è tantissima gente che è felicissima di essere interrotta per sapere che in quel momento, mentre sta navigando, anche i suoi amici sono collegati alla Rete. Fa sentire meno soli nel grande mare delle informazioni?

Se non siete orsi solitari come me e vi piacciono le sorprese e gli incontri inaspettati, allora quello che vi serve è un programma *ICQ*, che fa esattamente quello che ho descritto adesso: vi avvisa quando qualcuno che conoscete è in Rete contemporaneamente a voi. A proposito, tutti pronunciano

ICQ scandendo le lettere, ma andrebbe pronunciato all'inglese "*ai sic iù*" per rivelare il gioco di parole originale: la sigla suona come *I seek you*, cioè "io cerco te".

A dire il vero, ICQ (disponibile per Windows, Mac e qualsiasi apparecchio in grado di eseguire programmi Java presso http://www.icq.com) è soltanto il capostipite di tutta una serie di programmi analoghi: dopo di lui ne sono spuntati tanti altri, come Microsoft NetMeeting, Netscape CoolTalk, C6 di Tin.it, ma ormai tutti vanno sotto il nome di ICQ o, se volete un'espressione tecnica inglese, *buddy list* ("*bàddi list*").

L'idea fondamentale è semplice: questi programmi consentono di sapere chi è presente in Rete in un determinato momento e, se vi va, contattarlo. Mentre siete in Rete, i vostri amici possono sapere che state navigando e "venirvi a trovare", contattandovi tramite ICQ per scambiare quattro chiacchiere tramite computer. Se avete troppo da fare, potete comunque affiggere un cartello "Non disturbare".

Le idee semplici raramente rimangono tali a lungo, per cui al servizio di base se ne sono aggiunti molti altri: lo scambio di file (ICQ è molto in voga per scambiare musica digitale MP3), la navigazione in gruppo (ci si mette d'accordo su un sito da visitare tutti insieme), il gioco in Rete. Il tutto in tempo reale e mentre continuate la vostra normale esplorazione della Rete: ICQ è molto parsimonioso in quanto a uso delle risorse di Internet e del vostro apparecchio.

A ciascun utente che si abbona gratuitamente al servizio viene assegnato un *UIN* o *numero ICQ* che lo identifica (adesso sapete cosa significano quelle cifre che vedete spesso accanto agli indirizzi di e-mail) e che date alle persone dalle quali volete farvi contattare. Quando vi collegate a Internet e lanciate ICQ, il programma avvisa una serie di siti (chiamati *server ICQ*) del vostro arrivo in Rete. La notizia viene trasmessa immediatamente ai programmi ICQ dei vostri amici, se sono collegati, e a quel punto potete semplicemente essere lieti di sapere che qualcuno che conoscete è in Rete insieme a voi oppure distrarvi dalla vostra attività in Internet e mettervi a chiacchierare tramite la tastiera.

Ma qual è lo scopo di ICQ e simili? Se ve lo state chiedendo, avete una visione troppo tecnica di Internet. Ciò che conta, nella Rete, sono le persone, non le macchine. Lo "scopo" di ICQ è dar piacere alla gente. Il sommesso ma continuo lampeggiare della finestrella in un angolo dello schermo, che vi avvisa *"Marco si è collegato... Alice si è scollegata... Gianni è in Rete ma non vuole essere disturbato..."*, fa sentire Internet viva e pulsante. È lo stesso tipo di piacere che si prova andando a fare un giro in città e imbattendosi in un'amica. Due chiacchiere, un caffè, e poi di nuovo in pista, gratificati dalla sorpresa.

IRC e simili: pro e contro

Gli aspetti positivi di questo tipo di servizi rispetto alla normale telefonata sono chiaramente enormi, soprattutto quando si tratta di comunicare con persone all'altro capo del globo (o

semplicemente in un altro paese): il costo di una sessione di IRC a due è incomparabilmente minore di quello di una telefonata internazionale equivalente (e a volte anche di un'interurbana). Anche nel caso dell'uso in stile chat line, perlomeno non state spendendo 2.540 lire al minuto più IVA!

Un altro merito di IRC è che lascia una traccia scritta della "conversazione", e questo può essere utile a scopo di documentazione, sia per lavoro, sia per diletto. Se poi dovete comunicare in una lingua straniera, IRC ha il pregio di farvi vedere le parole invece di doverne decifrare i suoni, magari alterati dalla linea internazionale e dal terrificante accento del vostro interlocutore.

C'è anche un aspetto socialmente significativo di IRC: è uno degli strumenti di dialogo telematico maggiormente utilizzati dai sordi e dagli handicappati fisici. Su Internet ci sono molte persone che hanno scelto la telematica perché non possono usare il telefono per comunicare, ed è facile avere dialoghi anche molto lunghi con un disabile senza accorgersene, il che contribuisce senz'altro al loro inserimento nella vita quotidiana.

Può essere affascinante potersi sedere in un "salotto virtuale" (a volte, su alcuni canali piuttosto piccanti, sarebbe più giusto chiamarlo "camera da letto virtuale" a più piazze) e dialogare con persone di tutto il mondo. Accanto a discussioni molto tecniche e serie, nell'IRC ci sono canali dedicati ad argomenti stravaganti e alle lingue più strane, compresi il Klingon e l'Esperanto.

Purtroppo, però, il livello medio delle conversazioni tende ad essere piuttosto basso: inoltre i messaggi dei vari partecipanti arrivano accavallati e con un certo ritardo, ed è quindi molto difficile tenere il filo dei discorsi. Vale comunque la pena fare qualche esplorazione.

Molte delle "conversazioni" hanno un carattere piuttosto intimo, e molto si è detto nella stampa a proposito di quello che succede in queste aree di "sesso virtuale". In realtà, a parte il fatto che tutto avviene a livello puramente verbale (niente immagini, né tanto meno sospiri eloquenti), in queste aree non succede granché, e la confusione dei messaggi è notevolissima. Gente che arriva, gente che viene buttata fuori, gente che s'incontra e si scambia pettegolezzi tutto sommato piuttosto irrilevanti, ragazzini che fingono di essere donne e altri uomini che ignari fanno loro la corte... c'è di tutto.

Conversazioni a rischio

Le aree di chat di Internet sono ambienti pericolosi se non adottate un minimo di prudenza. L'ICQ e l'IRC, ad esempio, può essere utilizzato per recapitarvi un virus. Non accettate *mai* allegati tramite questi servizi; anzi, disattivate l'eventuale accettazione automatica presente in molti programmi. Se proprio dovete scambiare file con qualcuno, eseguite un controllo con un programma antivirus aggiornato.

Mi spiace dover tornare ancora una volta sull'argomento, ma se siete del gentil sesso, non adottate un nickname che lo riveli, specialmente nei canali di IRC più frivoli.

Cosa ancora più importante, state molto attenti a dare in giro il vostro vero nome, indirizzo o numero di telefono alle persone che ve li chiedono in Rete. C'è molta gente molesta là fuori (Internet rispecchia il mondo reale). Liberarsi da uno scocciatore telefonico è difficile e costoso. Trovarselo sotto casa è anche peggio.

Internet come cassaforte

Di recente è esplosa la mania dei siti che offrono spazio per custodire sulla Rete i file degli utenti. Alcuni dei più quotati sono *Docspace* (http://www.docspace.com), *@Backup* (http://www.atbackup.com), *Idrive* (http://www.idrive.com), *Free Disk Space* (http://www.freediskspace.com) e *Freedrive* (http://www.freedrive.com).

Il loro servizio è analogo a quello di una banca con le sue cassette di sicurezza: vi viene concesso un certo quantitativo di spazio in cui mettere sotto chiave quello che desiderate, per poi prelevarlo quando vi serve. Nel caso del servizio Internet, ovviamente, potete mettere al sicuro file di qualsiasi tipo e la chiave è una password, e non occorre recarsi fisicamente alla banca: si può fare tutto via Internet.

Volendo, la vostra "cassetta di sicurezza" può essere cointestata: basta dare la password alle persone che volete autorizzare. Se siete spiriti liberi e volete depositare dati da mettere a disposizione di chiunque, potete disattivare del tutto la password.

Intendiamoci: questi siti non hanno nulla a che vedere con quelli che ospitano le pagine Web. I siti-cassaforte ospitano soltanto file separati e individuali da depositare e prelevare, che non possono essere visualizzati durante la connessione come invece avviene per le pagine pubblicate presso i siti Web.

Ci sono vari motivi per usare un sito-cassaforte:

- **la sicurezza contro furti e disastri**. Potete depositare presso questi siti una copia dei vostri dati più importanti (la contabilità, ad esempio). Se il vostro ufficio viene devastato dai ladri o da un incendio, è probabile che le normali copie di sicurezza periranno nel disastro insieme al computer perché sono conservate nello stesso edificio. Normalmente, per evitare questo problema si deve fare una copia dei dati su dischetti o CD e poi portarla fisicamente altrove. Questi siti consentono di evitare questo rituale: standovene in ufficio potete depositare al sicuro una copia dei vostri dati all'altro capo del mondo.
- **la condivisione dei file**. Se dovete far avere un file a un gruppo di persone, potete spedirlo a uno di questi siti-cassaforte e poi invitare ciascuna persona a prelevarlo quando le è più comodo. Questo evita di pasticciare con gli allegati dell'e-mail, che fra l'altro non possono superare determinate dimensioni, mentre in un sito-cassaforte potete depositare file enormi senza alcun problema.
- **il dischetto virtuale**. Molti set top box, computer ultraportatili e sistemi informatici

aziendali non hanno unità per registrare dischetti, per cui non potete prelevare dati da questi apparecchi, né usarli per ricevere file da Internet. Potete però spedire un file a un sito-cassaforte, sicuri che nessun altro potrà prelevarlo, e poi consultarlo da casa o da un altro computer.

- **il servizio universale**. Essendo servizi accessibili tramite Web e utilizzabili con qualsiasi browser, i siti-cassaforte sono a disposizione di qualsiasi apparecchio collegabile a Internet, a prescindere da marca, modello e sistema operativo. In un medesimo sito potete conservare file per Linux, programmi per Windows, dati per un'agendina elettronica e i parametri del vostro miglior punteggio in un videogame.
- **l'archivio centrale**. Se viaggiate molto o se usate molti computer differenti, potreste memorizzare i file di uso più frequente nel sito-cassaforte, così potrete consultarli da qualsiasi apparecchio collegato a Internet.

La velocità è per ora uno dei fattori limitanti di questi servizi. Depositare o prelevare grandi quantità di dati da queste casseforti digitali alla velocità di un normale modem richiede una quantità di tempo esasperante. Le cose migliorano se avete un accesso diretto alla Rete, ma anche così è un procedimento piuttosto lungo.

C'è anche la questione della sicurezza: se depositate nel sito-cassaforte dati delicati, come un diario o la vostra contabilità, è meglio essere certi che nessun altro possa vederli. Questi siti in genere hanno delle politiche di sicurezza molto serie, ma se volete essere blindati a dovere è meglio imparare un po' di crittografia. Inoltre non tutti i siti si impegnano a conservare i vostri dati indefinitamente: leggete bene le avvertenze, perché potrebbero specificare che dopo un certo periodo trascorso senza che usiate il servizio (e senza quindi sorbirvi la pubblicità che alimenta il sito) la vostra "cassetta di sicurezza" verrà cancellata.

Un tuffo all'indietro

Questi sono soltanto alcuni degli strumenti supplementari per arricchire la vostra esperienza in Rete. Sono tutti molto colorati, animati, interattivi: sono anche tutti molto ingombranti, sia come dimensioni fisiche sul vostro disco rigido, sia come appetito di potenza di calcolo.

Ma la Rete non è sempre stata così affamata di superprocessori: come si viveva in Internet prima dell'epoca dei Pentium? Questo è l'argomento del prossimo capitolo.

Letture consigliate

Succedono davvero le storie d'amore e di passione via Internet raccontate dai giornali? Se volete scoprire gli insoliti e inquietanti meccanismi psicologici che si innescano fra due persone che comunicano soltanto tramite parole sullo schermo, senza mai vedersi né sentirsi, nelle aree di chat italiane di Internet, provate l'esperienza vissuta di Marina Bellini, esperta del lato umano della Rete,

descritta in *Maschi virtuali* (Apogeo) e nel relativo sito (http://www.maschivirtuali.com). Alcune trascrizioni dei dialoghi via Internet sono molto esplicite, ma il contesto lo esige.

9. Internet vecchio stile

Anche se il Web è la parte più vistosa ed emergente della Rete, non è *tutta* la Rete. Là fuori, nel ciberspazio, c'è un'enormità di materiale che non è e non sarà mai convertito allo standard chiassoso del Web. È tutto materiale che sfugge completamente alle normali ricerche. Per scovare questi tesori bisogna fare dell'archeologia informatica e tornare a usare gli strumenti antichi di Internet.

Queste pietre di selce digitali sono ancora perfettamente utilizzabili per una ragione molto semplice: quasi tutti i moderni servizi di Internet poggiano ancora sulla stessa struttura di comandi, creata ormai trent'anni fa, su cui poggiava la Rete anche prima dell'esplosione del Web. Per molti versi, i vari programmi odierni non fanno altro che abbellire e automatizzare questi vecchi comandi. Per fare un esempio, con una serie di comandi "vecchio stile" si può spedire un e-mail senza usare un programma mailer. Sono questi i comandi che consentono agli esperti della Rete di fare cose apparentemente impossibili: se volete diventare bravi hacker, è da qui che dovete cominciare a studiare.

Telnet

Prima del boom dei personal computer c'erano i *terminali.* Erano poco più che una tastiera e uno schermo: il processore non c'era, o per meglio dire ce n'era uno solo centralizzato, situato altrove, che veniva condiviso da diversi di questi strani apparecchi. Si vedono ancora in alcune piccole aziende a corto di soldi per aggiornarsi e in certi uffici pubblici, polverosi testimoni dell'arretratezza dell'amministrazione in Italia (*"mi spiace, il suo certificato non è ancora pronto... sa, il terminale non funziona..."*).

Il comando Telnet trasforma il vostro computer in uno di questi dinosauri, come se foste seduti davanti a un vero terminale del computer remoto al quale vi collegate. A seconda del livello di accesso che vi viene concesso, ad esempio, potete interrogare il computer alla ricerca di informazioni oppure far eseguire programmi che risiedono su quel computer e che non sono compatibili con il vostro (che so, far eseguire un programma per Unix da un supercomputer remoto e vederne i risultati sullo schermo del vostro televisore, collegato a Internet da un set top box o da una console per videogiochi).

Ma a cosa serve "rimbecillire" temporaneamente un computer? Lo spiego subito. Moltissimi grandi computer tuttora in funzione usano standard tecnici definiti decenni fa: solo testo, senza immagini, e niente mouse. Per dialogare con uno di questi antichi cervelloni occorre fargli credere che il nostro computer sia un normale terminale che rispetta quegli standard tecnici. Nel gergo informatico, questo tipo di finta si chiama *emulazione di terminale*. Il comando Telnet si occupa appunto di "emulare" un terminale: fa credere al computer remoto che il vostro super-Pentium III sia una bagnarola.

Naturalmente non esiste un solo tipo di emulazione di terminale: la vita sarebbe troppo facile. L'emulazione più frequente su Internet, soprattutto quando c'è di mezzo Telnet, si chiama *VT100*. Se il vostro programma per Telnet offre la possibilità di emulare questo tipo di terminale, attivatela.

Funzionamento in breve

Telnet è disponibile sia come comando, sia come programma, praticamente in tutti i sistemi operativi. In Windows, ad esempio, è disponibile sotto forma di un programma chiamato, guarda caso, *Telnet*.

Il procedimento per collegarsi a un sito tramite Telnet varia da computer a computer, ma la sostanza è questa: dopo aver stabilito la connessione a Internet, avviate il vostro programma Telnet (o date il comando *telnet*) e immettete il nome del sito che volete raggiungere, eventualmente seguito dal numero della sua *porta*.

Ogni sito è infatti raggiungibile passando per varie porte che corrispondono in genere a modalità di entrata differenti. Ad esempio, raggiungendo uno stesso sito attraverso porte diverse può capitare che non venga chiesta la password, o che si acceda ad un tipo di servizio non disponibile se si passa dalle altre porte.

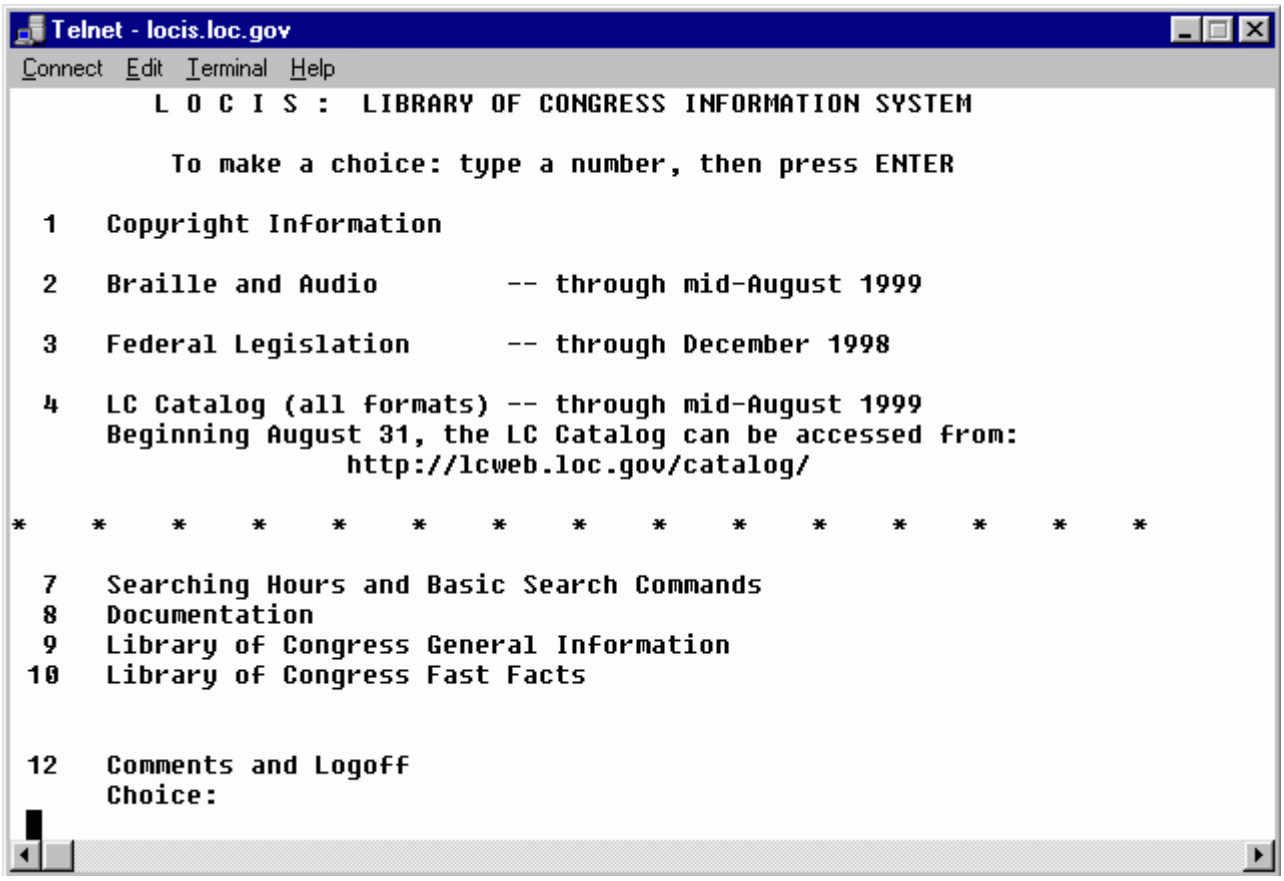
Se volete collegarvi ad un sito per usarne la funzione Telnet, vi conviene usare la porta 23, che in genere è comunque quella assegnatavi per default. Un altro tipico esempio di porta riservata è la 13, che si chiama *daytime port* perché consente di ottenere l'ora locale del sito raggiunto. Non è di utilità vitale per l'utente comune, ma può fare comodo quando occorre rispettare gli orari di disponibilità dei servizi e non si ha la più pallida idea di che ora siano nel paese con il quale ci si collega o quando il nome del sito non permette di identificarne la collocazione geografica. In Internet serve per tenere sincronizzati fra loro i vari computer della Rete.

Con tutta probabilità vi verrà chiesto un nome di login: di solito è una formalità (al punto che il nome da immettere compare nel messaggio iniziale di benvenuto), a meno che visitiate un sito privato, nel qual caso vi verrà chiesta anche una password.

E a questo punto siete "entrati" nel computer remoto.

Pronti alla fuga!

A volte, a causa del traffico o dell'imperfetto funzionamento di alcuni programmi residenti su siti lontani, il collegamento ad un certo punto si blocca e non succede più nulla. Tenete presente, comunque, che la risposta dei siti Telnet è proverbialmente lenta. Abbiate molta pazienza prima di scollegarvi.



Una sessione con Telnet in Windows: siamo diventati un terminale dell'immensa Biblioteca del Congresso americana.

Non vi preoccupate: non avete mandato in tilt il computer remoto, che ripristinerà la situazione non appena avrà tempo di gestirla. Il guaio è che mentre magari il computer remoto può mettersi con comodo a chiudere la vostra sessione quando gli pare, voi siete in collegamento telefonico con il vostro fornitore d'accesso e la bolletta telefonica continua ad aumentare intanto che il vostro computer è "congelato" in attesa della reazione del cervellone remoto.

In casi come questi conviene terminare la sessione in modo brutale, digitando il *carattere di escape ("eschèip")*. Questo carattere è una "via di fuga" predisposta dal computer remoto per permettervi di disimpegnarvi quando le cose vanno storte.

In genere il carattere di escape è *Ctrl-]*. In altre parole, si preme il tasto Ctrl, lo si tiene premuto e si preme una sola volta il tasto della parentesi quadra chiusa. Se le parentesi quadre sulla vostra tastiera italiana si digitano premendo AltGr più il tasto delle parentesi quadre, la combinazione di tasti diventa triplice: Ctrl-AltGr-parentesi quadra chiusa. Un bell'esercizio per le dita, vero?

Quando vi collegate ad un sito con Telnet, fra le prime avvertenze visualizzate sul vostro schermo dal computer remoto troverete quasi sempre l'indicazione del carattere di escape. Prendetene nota in modo da poter concludere la sessione in caso di necessità. Nei casi peggiori, potete sempre chiudere brutalmente il vostro programma Telnet: la connessione al computer remoto cadrà (quella a Internet no). Non fatelo se non è indispensabile: è cattiva Netiquette

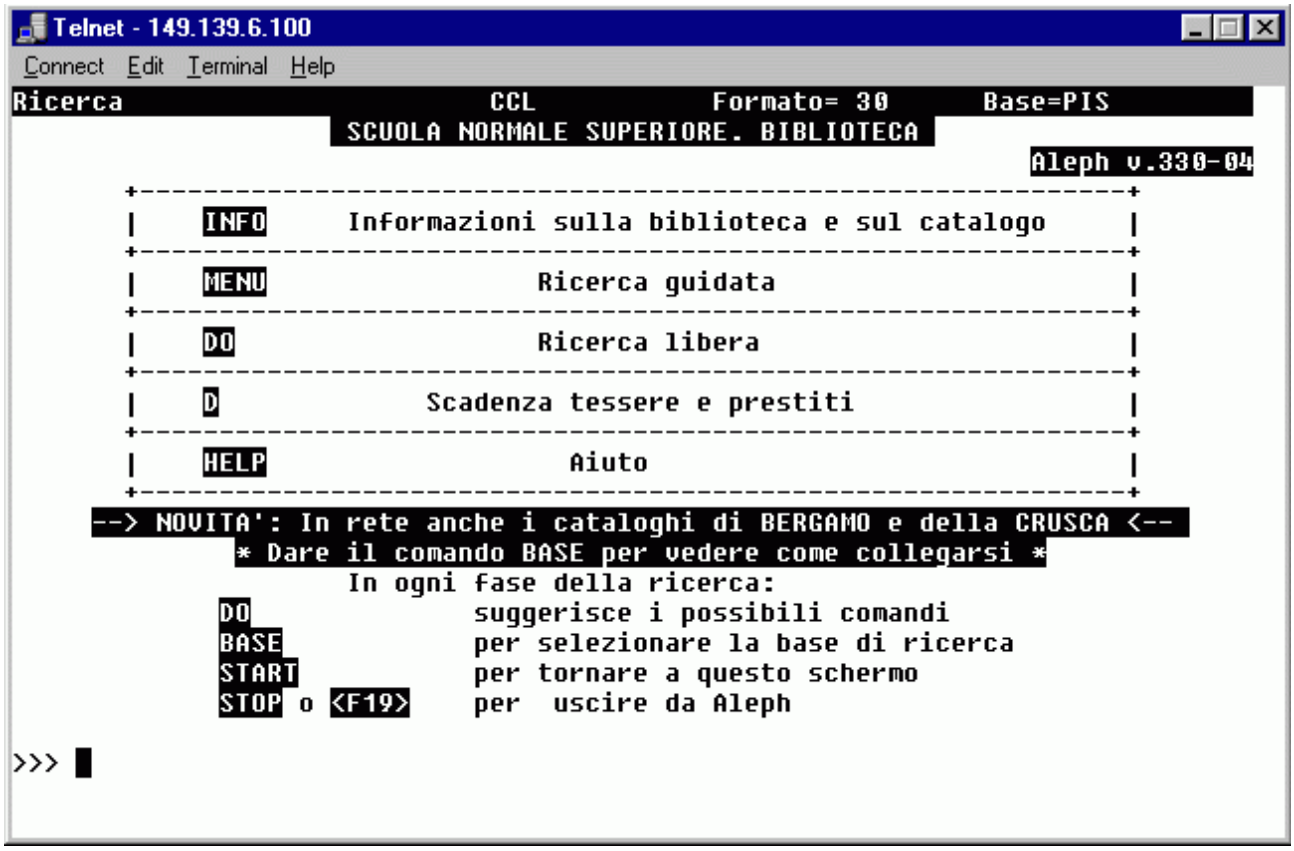
Attenzione, inoltre, a non toccare i tasti funzione della vostra tastiera intanto che siete alle prese con un collegamento Telnet! Le funzioni assegnate ai vostri tasti funzione possono non coincidere (anzi, quasi sicuramente non coincidono) con quelle del computer remoto al quale siete collegati. Tasti come Ins, Canc, e Backspace possono funzionare in modo diverso sul vostro computer e sul computer remoto.

Ricordate sempre che durante una sessione Telnet il vostro computer è semplicemente un terminale del computer remoto e nulla più: ciò che vedete sullo schermo è l'interpretazione delle vostre digitazioni eseguita da quest'ultimo e non dalla vostra macchina. Anche le combinazioni di tasti (Ctrl o Alt più un altro tasto) possono avere effetti imprevedibili.

Molti degli usi più stimolanti di Telnet esulano dalla portata di questo libro: come dicevo, è uno dei comandi da padroneggiare per diventare veri esperti manipolatori della Rete. Ma con tutto il dovuto rispetto per voi, prima di cominciare a lavorare con questi strumenti è meglio che vi studiate un bel po' di documentazione assai più tecnica di questo testo introduttivo. Ricordate cos'è successo a Topolino apprendista stregone in *Fantasia*? Appunto.

Faccio comunque un paio di esempi giusto per darvi un assaggio di quello che si può combinare con Telnet. Usando questo servizio per collegarsi all'indirizzo 149.139.6.100, si raggiunge il sito Internet dell'Istituto Universitario Europeo (IUE). L'Istituto è presente anche come sito Web (presso http://www.iue.it), ma alcuni suoi servizi sono accessibili soltanto tramite Telnet. Ad esempio, da qui possiamo esplorare non solo la biblioteca dell'IUE, ma anche numerose altre importanti biblioteche italiane, come la Biblioteca Nazionale Centrale di Firenze e la Biblioteca della Scuola Normale Superiore di Pisa.

Da qui si può sapere se la biblioteca dispone di un determinato libro oppure fare ricerche bibliografiche in questi enormi archivi. Notate l'aspetto molto spartano della schermata: niente colori, niente grafica, solo testo: però, se provate a collegarvi, noterete anche che la schermata compare istantaneamente. Merito della parsimonia di Internet vecchio stile.



Accediamo a una biblioteca italiana tramite Telnet.

Prima che vi facciate l'impressione sbagliata, Telnet non è uno strumento esclusivamente per topi da biblioteca. Ad esempio, è utile se siete interessati ai newsgroup ma il news server del vostro fornitore d'accesso non offre un particolare newsgroup che vorreste seguire. In casi come questi dovrete ricorrere a un news server pubblico. Normalmente dovreste avviare il vostro newsreader, prelevare da ciascun news server la chilometrica lista dei newsgroup disponibili e poi sfogliarla per vedere se c'è quello che vi interessa. Una pizza, oltre che un salasso: ci vogliono diversi minuti di collegamento telefonico per prelevare ciascuna lista.

Entra in gioco Telnet. Basta lanciare Telnet specificando il nome del news server e (attenzione) la porta giusta, che in questo caso è la 119. Dopo i messaggi di benvenuto, digitate *group* seguito dal nome del newsgroup desiderato. Il news server vi risponderà subito dicendovi se quel newsgroup è disponibile o no. Comodo, vero?

Dietro le quinte dei siti italiani: whois

Se volete sapere chi gestisce un qualsiasi sito italiano o europeo, potete ricorrere ancora una volta a Telnet, che vi conduce a un'altra vecchia gloria di Internet: *whois*.

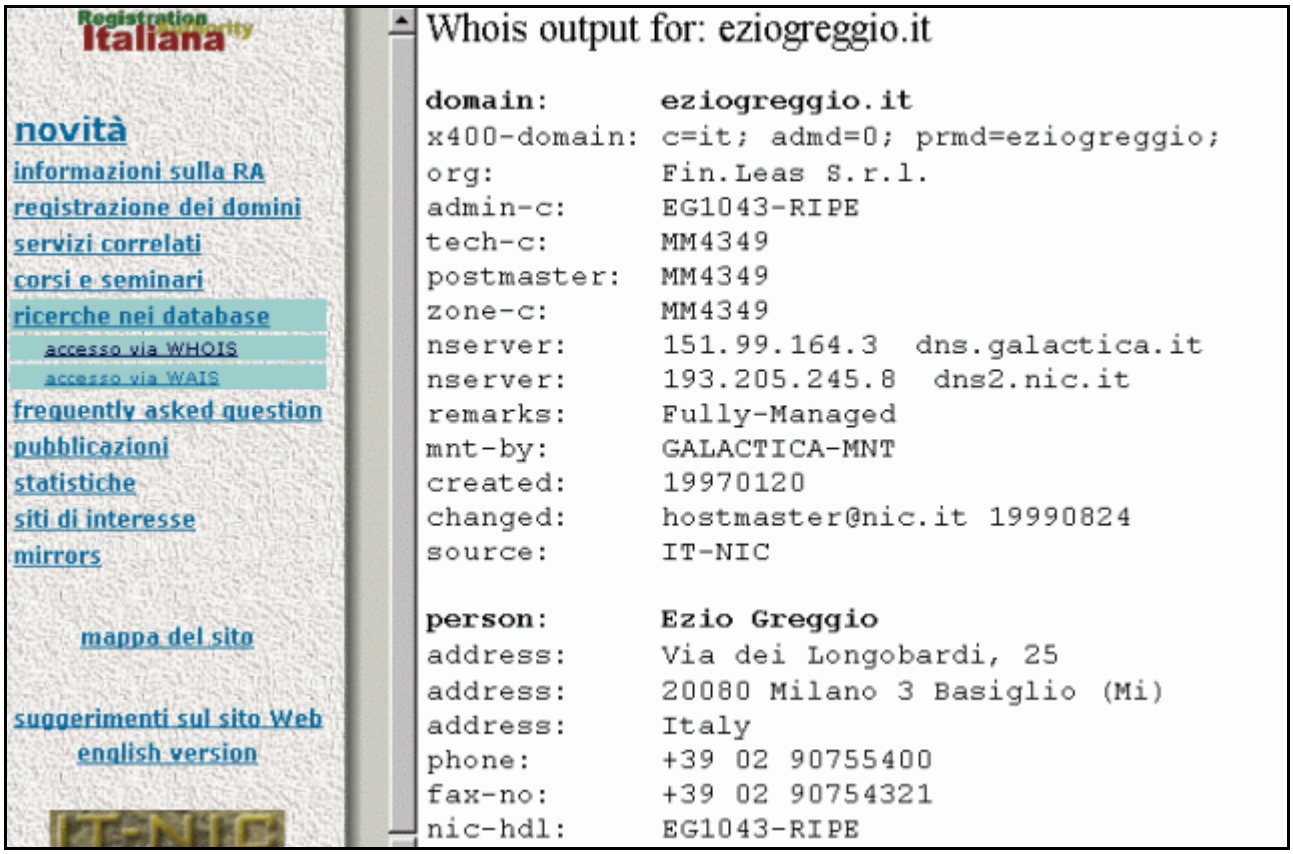
Sapere chi c'è dietro un sito non è semplice ficcanaseria. Spesso serve per evitare le truffe dei siti porno a pagamento oppure i "giochi di sponda" che molte società senza troppi scrupoli usano su Internet per pubblicizzarsi o per disseminare notizie false, oppure per risalire ai colpevoli delle peggiori interferenze nei newsgroup. Comunque sia, il procedimento è semplice: usate Telnet per raggiungere il sito whois.ripe.net, che è il centro di coordinamento Internet per l'Europa. Il sito vi mette automaticamente nelle sapienti mani di *whois*, che vi chiede di immettere il nome del sito sul quale volete maggiori informazioni. Tutto qui.

Ecco il risultato di una ricerca un po' curiosa: ho immesso *eziogreggio.it* come nome del sito. Fra l'altro la ricerca rivela, oltre ai dati della società che cura gli interessi Internet del conduttore di *Striscia la notizia*, un numero di telefono che non compare nell'elenco telefonico (sì, ho controllato), alla faccia della riservatezza. Ve lo dicevo, io, che siamo tutti schedati su Internet.

```
domain: eziogreggio.it
descr: Fin.Leas S.r.l.
admin-c: EG1043-RIPE
tech-c: MM4349
zone-c: MM4349
nserver: dns.galactica.it
nserver: dns2.nic.it
remarks: Fully-Managed
remarks: created: 19970120
mnt-by: IT-NIC
changed: hostmaster@nic.it 19990824
changed: hostmaster@nic.it 19990825
source: RIPE
person: Ezio Greggio
address: Via dei Longobardi, 25
address: 20080 Milano 3 Basiglio (Mi)
address: Italy
phone: +39 02 90755400
fax-no: +39 02 90754321
nic-hdl: EG1043-RIPE
changed: domain@galactica.it 19990824
changed: hostmaster@nic.it 19990825
source: RIPE
person: Matteo Mangiacavalli
address: GALACTICA S.p.A.
address: Via Tonale, 26
address: 20125, Milano
address: Italy
phone: +39 02 676201
fax-no: +39 02 67076401
```

```
e-mail: matteo@galactica.it
nic-hdl: MM4349
notify: matteo@galactica.it
mnt-by: GALACTICA-NOC
changed: hostmaster@nic.it 19980818
changed: hostmaster@nic.it 19980825
changed: sysalt@galactica.it 19990514
source: RIPE
```

In effetti la stessa ricerca si può effettuare tramite il Web, anche se ci vuole il triplo del tempo: per i siti italiani ci si collega col proprio browser a http://www.nic.it/RA/database/viaWhois.html, per quelli europei (Italia inclusa) il sito è http://www.ripe.net/db/whois.html. Lì trovate un servizio che converte i risultati di *whois* in pagine Web.



Una ricerca per sapere chi sta dietro un sito Internet italiano.

Chi controlla Internet?

Nei capitoli precedenti ho accennato al fatto che Internet non ha un centro, un singolo proprietario o un direttore generale. Tuttavia ci sono alcuni organi di amministrazione tecnica che sovrintendono allo sviluppo

della Rete e al suo buon funzionamento. Visto che ho parlato di centri di coordinamento da consultare per sapere a chi appartiene un sito, colgo l'occasione per citare alcune delle principali organizzazioni che formano il "governo illuminato" di Internet.

- La manutenzione e l'evoluzione del TCP/IP, il protocollo di comunicazione creato da Vinton Cerf che è il pilastro di tutta Internet, sono affidate all'*Internet Engineering Task Force*, consultabile presso http://www.ietf.org. Questo gruppo, insieme all'*Internet Architecture Board* (IAB), definisce inoltre gli standard della Rete, sotto forma di documenti chiamati *RFC* (dalle iniziali di *Requests for Comments*). Se volete sapere ogni più piccolo dettaglio sul funzionamento di Internet, attingete agli RFC.
- Gli standard per il Web, invece, sono definiti dal *World Wide Web Consortium* (http://www.w3.org). Qui lavora Tim Berners-Lee, l'inventore di protocolli di base del Web come l'HyperText Transport Protocol (HTTP). Il Consortium definisce anche gli standard e le evoluzioni della struttura delle pagine Web scritte in HTML.
- Internet non è amministrata soltanto da ingegneri: il lato umano e sociale della Rete, con le sue implicazioni in fatto di sicurezza, riservatezza e libertà d'informazione, sono in gran parte coordinate dalla Internet Society (http://www.isoc.org). Chiunque può far parte di questa organizzazione senza scopo di lucro, che molti chiamano l'"anima collettiva" di Internet. Il "braccio armato" delle questioni morali in Rete è la *Electronic Frontier Foundation* (http://www.eff.org), che combatte a suon di cause coi più grandi nomi dell'informatica e dei governi (compreso quello italiano) in favore della libertà di espressione sulla Rete.
- E poi ci siete voi, sotto vari aspetti. Nel vostro piccolo, se avete pagine Web, se pubblicate informazioni in Rete o se partecipate a un newsgroup, "controllate" una parte di Internet; minuscola, forse, ma significativa: influenzate altre persone. Come consumatori, come utenti della Rete, come sostenitori della libertà di pensiero e magari come genitori preoccupati per quello che i figli possono trovare in Rete, fate scelte che sommate a quelle di tanti altri come voi plasmano Internet e ne decidono il corso futuro. Il Web non esisterebbe se gli utenti non avessero cominciato a riempirne il vuoto con passione affiggendovi le loro pagine.

Ricerca di file negli archivi FTP: archie

La marea di file presenti su Internet è talmente enorme, e sono così numerosi i siti da esplorare, che trovare il programma o il documento che c'interessa è come cercare il classico ago nell'ancor più classico pagliaio. I motori di ricerca non sono molto utili per queste cose, anche perché di solito "vedono" soltanto le pagine Web. I colossali archivi accessibili tramite FTP sfuggono quasi sempre alla loro esplorazione.

A questo problema pone almeno in parte rimedio *archie* (si pronuncia "*arci*"). In sostanza, questo servizio esplora periodicamente tutti i siti Internet che offrono accesso per il prelievo di file tramite il servizio *FTP* (descritto nel Capitolo 8) e crea un grande elenco del contenuto di questi siti. Chiunque può così collegarsi ad un sito Internet presso il quale risiede una copia di questo archivio e cercare l'ubicazione esatta di quello che gli serve.

Archie è disponibile sia come programma da installare sul vostro computer, sia come comando da digitare durante una sessione Telnet presso appositi *siti archie* (a proposito, per motivi che sicuramente vi annoierebbero a morte, *archie* va scritto minuscolo, anche se è un nome proprio).

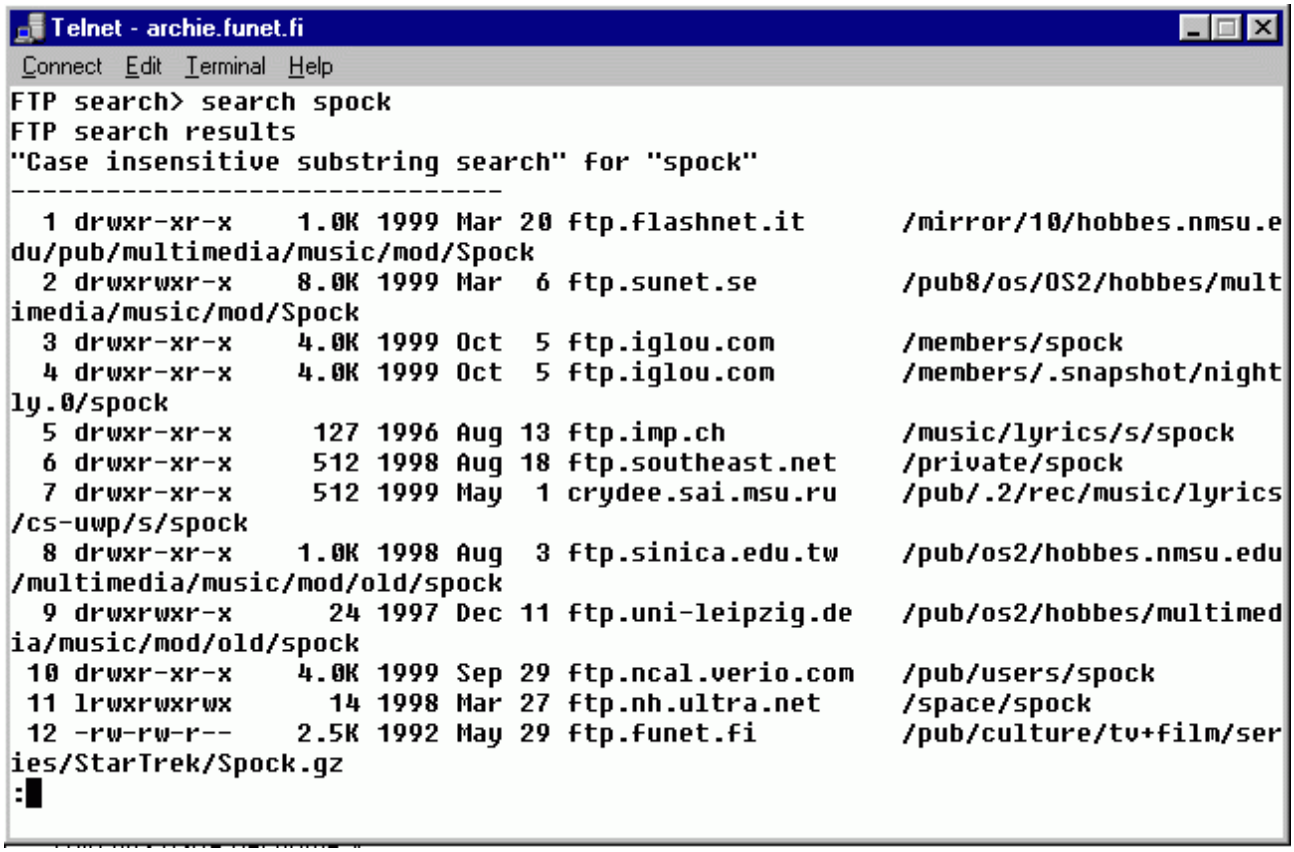
I programmi per archie (tecnicamente si chiamano *client*) da installare sul vostro computer sono

molto più facili da usare della versione Telnet, perché automatizzano tutto il procedimento di consultazione, ma hanno appunto il difetto che bisogna procurarseli, installarli e configurarli. Se tutto quello che vi serve è una ricerca occasionale, potete fare a meno di tutte queste tribolazioni e usare il Telnet che avete con tutta probabilità bell'e pronto sul vostro apparecchio.

Il primo passo è, logicamente, collegarsi alla Rete e poi usare il programma Telnet per raggiungere uno dei siti che offrono il comando archie. In effetti archie è presente quasi ovunque, ma sono pochi i siti che ne offrono l'uso pubblico, vale a dire gli *archie server pubblici*. Come molte cose di Internet, anche la lista degli archie server pubblici cambia in continuazione: per mantenerla aggiornata conviene usare un motore di ricerca e immettere *archie server* e *public* come parole da ricercare. Qui ne posso citare almeno uno, quello "storico" archie.funet.fi che dalla Finlandia offre al mondo uno dei più vasti archivi di dati e programmi per ogni sorta di computer.

Una volta collegati, vi verrà chiesto di digitare un nome d'utente che in genere è *archie*. Se c'è da immettere una password, questa sarà specificata nella schermata iniziale del collegamento. Fatto questo, basta seguire le istruzioni che compaiono sullo schermo per interrogare l'elenco dei file contenuti nei siti FTP di tutto il mondo. Se non sapete che pesci pigliare, potete sempre provare a digitare *help*: otterrete l'elenco dei comandi disponibili e una loro breve spiegazione (d'accordo, è in inglese, ma non si può avere tutto nella vita).In genere l'operazione è abbastanza semplice: si digita *prog* o *search* seguito dal nome del file che cercate. Potete indicare anche solo una parte del nome. A dire il vero, archie ha un'infinità di parametri che non è il caso di spiegare qui. Li trovate senz'altro spiegati presso il server archie o in uno dei tanti manuali "per esperti" reperibili su Internet.

La risposta dell'archie server sarà un'elencazione più o meno lunga di tutti i siti FTP del mondo che contengono file corrispondenti al vostro criterio di ricerca. L'elencazione precisa non solo il nome del sito FTP ma anche la cartella (più propriamente, la *directory*) che contiene il file che state cercando. Basterà usare CuteFTP o un altro programma analogo per andare a recuperarlo a colpo sicuro.



Una sessione archie presso un server finlandese e il risultato dell'interrogazione.

C'è ma non si vede, o si vede ma non c'è?

Archie effettua la scansione delle directory di Internet con una certa periodicità, non in tempo reale. Pertanto la situazione indicata nei database di archie può non corrispondere a quella effettiva in un dato momento presso un determinato sito.

Ad esempio, se il gestore del sito cancella un file appena dopo che archie ha eseguito la sua scansione, archie continuerà a dirvi che quel file esiste, mentre in realtà non c'è più.

Asterix, Obelix e... Unix??

Unix (pronunciato *"iùnics"*) è il sistema operativo usato da quasi tutti i computer che fanno da nodi per Internet. Nelle vostre scorrerie elettroniche con Telnet, prima o poi vi imbatterete in un sito remoto che vi risponde soltanto con uno schermo vuoto che attende un vostro comando. Avete trovato Unix.

Unix è fatto così: si aspetta che voi sappiate cosa fare e non abbiate bisogno di suggerimenti. In casi come questi è importante avere almeno un'infarinatura sul funzionamento di Unix. Fra l'altro, visto lo strabiliante successo dei sistemi operativi alternativi a Windows, e in particolare del già citato *Linux* (una versione liberamente distribuibile di Unix), conoscere un po' di Unix è tornato ad essere importante per la vita informatica sia in Internet che sul proprio personal computer.

Giuro che ho fatto di tutto per risparmiarvi di dover imparare Unix, ma qualcosina almeno dovreste conoscere. Se già sapete usare Unix, o se giurate di non usare mai il servizio Telnet per comandare a distanza computer che usano Unix o simili, saltate pure questa sezione.

Se già usate o avete usato il sistema operativo DOS, Unix non dovrebbe esservi particolarmente ostico: i concetti di base sono molto simili, tant'è vero che si potrebbe quasi dire che il DOS è il parente povero di Unix (con buona pace di Bill Gates e della sua Microsoft). Ci sono però due differenze fondamentali:

- il comando *cd* esiste in Unix come in DOS, ma funziona in modo diverso, il che è l'ideale per mandarvi in confusione.
- A differenza del DOS e di Windows, Unix distingue fra lettere maiuscole e minuscole.

Se venite dal mondo Macintosh o da Windows 95/98, dovrete abituarvi anche al concetto di *directory*, che è l'equivalente Unix delle cartelle dei Mac e di Windows. Chi ha usato il DOS o Windows 3.1 si ricorderà che le cartelle si chiamavano già *directory*, quindi il problema non si pone.

Le directory sono organizzate secondo una struttura ad albero: al livello più alto c'è la directory principale, o *root directory* (*"rùut dàirectory"*), e "sotto" di essa ci sono le *subdirectory ("sàbdairectory")*, che a loro volta possono contenere delle ulteriori subdirectory (così come le cartelle possono contenere altre cartelle).

I comandi Unix indispensabili

Spiegare Unix in un paio di pagine è come spiegare la politica italiana ad uno straniero: semplicemente impossibile. Qui posso descrivervi brevemente soltanto alcuni dei comandi che potrebbe capitarvi di dover usare.

- **cat**. Questo comando equivale al comando DOS *type*. Per visualizzare un file sullo schermo facendogli fare una pausa ogni volta che si riempie lo schermo, digitate **cat *nomefile* | more**. Per interrompere la visualizzazione del file potete premere Ctrl-C.
  Il comando **cat** si può usare anche per scrivere o trasmettere un file di testo, in modo analogo al comando DOS *copy con*. Ad esempio, se digitate **cat > pippo** e avete le debite autorizzazioni, create un file di nome **pippo** sul computer al quale siete collegati; quello che

digitate viene registrato in quel file. Per terminare la registrazione e chiudere il file digitate Ctrl-D.

- **cd**. Croce e delizia per gli utenti DOS, questo comando consente di passare da una directory all'altra. Per ottenere questo risultato digitate **cd** seguito dal nome della directory di destinazione.
  Attenzione: a differenza del DOS, il comando **cd** di Unix usa la barra normale (il simbolo /) al posto della barra rovescia o *backslash* del DOS (il simbolo \). Come nel DOS, se dovete risalire lungo la struttura ad albero delle directory, potete digitare **cd ..**
- **cp**. Questo comando serve per copiare un file. Il formato della sintassi è **cp *nomefile1* *nomefile2***, dove al posto di ***nomefile1*** e ***nomefile2*** immettete rispettivamente il nome del file di partenza, cioè quello da copiare, e il nome che volete assegnare alla copia. Se esiste già un file con il nome che assegnate alla copia, viene sovrascritto.
- **ls**. Questo è l'equivalente Unix del comando DOS *dir*, con l'aggiunta del fatto che elenca i file in ordine alfabetico. Aggiungendo il parametro **|more** (il carattere *pipe* seguito da *more*), l'elencazione dei file fa una pausa ogni 24 righe.
  Il comando **ls** non elenca i cosiddetti "file nascosti": per visualizzarli bisogna digitare il parametro **-a**. Il parametro **-l** elenca anche le dimensioni del file, espresse in byte, insieme alla sua data di creazione e di modifica.
- **mv**. Sotto DOS si usa il comando *rename*, che serve per cambiare il nome ad un file. In Unix si usa invece **mv**, con la sintassi **mv *nomedelfile nuovonome***. Questo comando cambia il nome del file indicato al posto di ***nomedelfile*** assegnandogli il nome specificato al posto di ***nuovonome***. Potete usarlo anche per spostare un file da una directory all'altra: basta specificare anche il nome della directory al posto di ***nuovonome***.
- **rm**. Questo comando Unix cancella un file. Basta digitare il nome del file da cancellare dopo questo comando.

Caratteri jolly di Unix

I nomi dei file Unix non risentono delle fastidiose limitazioni di lunghezza del DOS e di Windows 3.1 (Windows 95 e successivi consentono nomi lunghi, ma con regole diverse da quelle di Unix, alla faccia della compatibilità). Proprio per questo, a volte è scomodo dover digitare un nome di file chilometrico.

Il problema si risolve usando delle convenzioni, chiamate *caratteri jolly* o *wildcard* (*"uàil-càrd"*) per indicare i nomi in modo riassuntivo, un po' come si fa con il DOS e le varie versioni di Windows.

- *L'asterisco* si usa per indicare una porzione di qualsiasi lunghezza: ad esempio, il comando **ls pip*** elencherà tutti i file che iniziano per *pip*, come ad esempio *pippo*, *piperita.patty*, *pipppero* e così via.
- Il *punto interrogativo* invece sta a indicare un qualsiasi singolo carattere di un nome di file.

Ad esempio, **ls pip??** elencherà tutti i file il cui nome ha cinque lettere e in cui le prime tre sono *pip*, come ad esempio *pippo*, *pippi*, *pipio*, ma non elencherà *pipppero*.

Lunga è la strada e stretta la via: Traceroute

Concludo questa breve carrellata dei servizi Internet "vecchio stile" ancora utili anche nell'era del dominio del Web con un metodo per sapere quale strada percorrono i dati per andare dal vostro computer al sito che volete visitare.

Chissenefrega, direte voi: l'importante è che arrivino. Purtroppo non è così: se la strada che percorrono i dati è troppo lunga e tortuosa, o se è troppo stretta perché intasata di altri dati, il vostro viaggio in Internet sarà una tortura cinese. Per sapere come rimediare al problema bisogna scoprire dove c'è l'ingorgo.

Il comando *traceroute* (si pronuncia *"trèis-rùut"*) serve proprio a sapere quale percorso seguono i vostri dati nelle loro tappe da un sito Internet al successivo, fino a quello di destinazione. Usandolo, otterrete anche una scaletta dei tempi di percorrenza di ciascuna tappa.

È un'informazione molto utile per confrontare le prestazioni offerte dai vari fornitori d'accesso Internet. Sapendo leggere un traceroute, potete capire se la lentezza dei vostri collegamenti dipende dal vostro fornitore o dal resto di Internet.

Gli utenti di Windows dalla versione 95 in poi hanno la vita facile (almeno in questo caso): il comando traceroute è incorporato nel loro sistema operativo. Naturalmente trovarlo non è facile, anche perché non si chiama *traceroute*, come sarebbe sensato aspettarsi, ma *tracert*. Praticamente tutti gli altri sistemi operativi dispongono di traceroute sotto una forma o un'altra.

Se durante un collegamento a Internet avviate il servizio traceroute specificando l'indirizzo (letterale o numerico) di un sito Internet, otterrete l'elencazione del percorso seguito per raggiungere quel punto della Rete. Guardate questo esempio commentato di un traceroute che ho eseguito durante un mio soggiorno in Inghilterra per raggiungere il sito del fornitore d'accesso italiano Libero:

```
C:\WINDOWS>tracert libero.it
Tracing route to libero.it [193.70.192.18]
over a maximum of 30 hops:
```

Il servizio fornisce subito la conversione dell'indirizzo letterale nel suo corrispondente numerico; inoltre pone un limite al numero di *hop* (gli stessi "salti" che abbiamo visto nel Capitolo 5 a proposito dell'e-mail) ammessi per raggiungere la destinazione. Poi inizia il resoconto del viaggio digitale:

```
 1   128 ms   130 ms   385 ms  s07.ap07.dialin.global.net.uk
```

```
     [195.147.224.7]
 2   140 ms   136 ms   391 ms  fe1-0-llb-x-many.r2.ap07.dialin.global.net.uk
     [195.147.224.58]
 3   137 ms   131 ms   139 ms  fd2-0-llb-x-r-many.PS4.core.rtr.xara.net
     [195.147.242.97]
 4   132 ms   129 ms   119 ms  hs4-0-llb-x-ps4.HE4.core.rtr.xara.net
     [195.147.240.6]
 5   165 ms   137 ms   136 ms  hs4-0-1-llb-x-he4.HE2.core.rtr.xara.net
     [194.143.164.129]
 6   154 ms   137 ms   126 ms  fd5-0-0-llb-x-many.HE5.core.rtr.xara.net
     [194.143.163.115]
 7   134 ms   141 ms   116 ms  at9-0-0-2-llb-d2200-he5.TH1.core.rtr.xara.net
     [194.143.164.190]
 8   127 ms   147 ms   129 ms  linx1.teleglobe.net
     [195.66.224.51]
 9   147 ms   139 ms   132 ms  if-1-1-1.bb1.fft.Teleglobe.net
     [195.219.0.202]
10   151 ms   150 ms   150 ms  cust-gw.Teleglobe.net
     [195.219.64.166]
11   244 ms   230 ms   227 ms  ffm-145-253-0-128.arcor-ip.net
     [145.253.0.128]
```

Controllando l'indirizzo IP indicato nell'ultima riga salta fuori che siamo passati dall'Inghilterra direttamente alla Germania, il che è un po' strano, visto che i due paesi non confinano direttamente l'uno con l'altro. Nella strana logica di Internet, evidentemente, Belgio, Olanda e Francia non contano.

```
12   305 ms   339 ms   236 ms  ffm-145-253-0-140.arcor-ip.net
     [145.253.0.140]
13   251 ms   219 ms   222 ms  nbg-145-253-0-112.arcor-ip.net
     [145.253.0.112]
14   237 ms   235 ms   247 ms  mue-145-253-0-208.arcor-ip.net
     [145.253.0.208]
15   239 ms   308 ms   237 ms  mue-145-253-4-19.arcor-ip.net
     [145.253.4.19]
16   155 ms   157 ms   150 ms  145.253.8.46
17   159 ms   161 ms   401 ms  192.106.7.161
```

Ed eccoci finalmente in Italia: ancora una volta, fra l'altro, abbiamo scavalcato un paese (la Svizzera) e siamo sbarcati direttamente a Genova.

```
18   169 ms   171 ms   164 ms  gw3.iunet.it [192.106.1.145]
19     *      212 ms     *     151.5.212.131 [infostrada]
20     *        *        *     Request timed out.
21     *        *        *     Request timed out.
22     *        *        *     Request timed out.
23     *        *        *     Request timed out.
24     *        *        *     Request timed out.
25     *        *        *     Request timed out.
26     *        *        *     Request timed out.
27     *        *        *     Request timed out.
```

```
28      *         *         *      Request timed out.
29      *         *         *      Request timed out.
30      *         *         *      Request timed out.
```

E qui, purtroppo, cominciano i guai. I tempi di risposta dei siti italiani sono stati talmente lunghi che traceroute si è stufato di aspettare (è questo il significato di *request timed out*). La prova è stata condotta la sera tardi, quando il traffico Internet in Italia è molto intenso, e quindi le cose non stanno sempre così male; quello che conta in questo caso, però, è che ho scoperto dove sta il problema che causava il rallentamento del mio collegamento con i siti italiani. Il mio fornitore d'accesso in Inghilterra può dormire sonni tranquilli. Stavolta.

Il cimitero degli elefanti

Sono passati solo cinque anni dalla prima versione di *Internet per tutti* e la Rete è già irriconoscibile. Sfogliando le pagine di quell'ormai vetusto manuale ho trovato tanti servizi che ormai sono praticamente scomparsi, soppiantati dalla squillante grafica del Web.

In realtà dovrei intitolare questa sezione *Il cimitero delle pulci*, dato che questi servizi occupavano uno spazio infinitesimo, e richiedevano computer drasticamente meno potenti, rispetto ai loro equivalenti moderni.

Certo, la Rete adesso è più facile da usare. Ma permettetemi di salutare brevemente e con nostalgia i comandi e i servizi che costituivano un tempo la spina dorsale di Internet e consentivano quelli che all'epoca sembravano miracoli. Li troverete ancora in giro per Internet, ma la loro utilità ormai sta svanendo.

- **WAIS, Veronica, Hytelnet, Gopher** sono i nonni dei motori di ricerca attuali. Ci sono ancora molti siti Internet che funzionano con questi programmi ma sono stati resi accessibili tramite un browser: la ricerca di informazioni sui siti italiani che abbiamo visto prima usa infatti WAIS.
- **Talk** era l'antico equivalente dell'Internet Relay Chat; forse lo usa ancora qualche sito universitario.
- **Pine, elm** e soci erano l'unico modo per gestire l'e-mail quando tutta Internet funzionava tramite Telnet: bisognava leggersi la posta durante i collegamenti (e questo, nostalgia a parte, era costosissimo).
- **Ping** è ancora in uso fra gli esperti, ma ormai è di poco interesse per l'utente medio: serviva per verificare l'esistenza di un indirizzo di un utente o di un sito. Può essere un'alternativa più concisa al traceroute per la ricerca dell'indirizzo numerico corrispondente a un dato indirizzo letterale.
- **Finger** restituisce un file di testo contenente le informazioni che l'utente desidera diffondere in Rete; il guaio è che nessuno redige più il file in questione e quindi la sua utilità sta sfumando.

Proseguire oltre con questa rassegna di *zombie* telematici non mi pare una buona idea: non vorrei intristirvi troppo. Potete tuttora trovare in Rete ottimi manuali che spiegano come usarli, se vi incuriosiscono, ma vi assicuro che ormai potete vivere benissimo in Internet senza conoscerli.

Ma attenti: a volte ritornano!

10. Privacy e sicurezza

Internet è uno strumento pericoloso. Non nel senso morale in cui lo intendono i giornalisti, che credono che il pericolo della Rete stia nella disponibilità abbondante, immediata e gratuita di corpi nudi, ma nel senso pratico e tangibile in cui lo è un coltello se viene messo nelle mani di chi non è stato preparato a maneggiarlo.

Vedo che gli utenti entrano in Rete con troppa fiducia verso gli strumenti che usano per interagire con Internet. Credono che il coltello non possa ferire loro le dita. Diamine, il fabbricante l'avrà reso conforme ai migliori standard di sicurezza, no?

No.

Probabilmente pensate che io stia esagerando. Ne riparleremo dopo che avrete letto questo capitolo. Nel frattempo, considerate questi piccoli fatti:

- Nei pochi mesi da quando è stato messo in circolazione, Internet Explorer 5, uno dei browser più diffusi, ha già rivelato almeno tre difetti di programmazione gravi al punto che è sufficiente visitare una pagina Web per consentire a un utente ostile di leggere il contenuto del vostro computer. E questa è la *quinta* versione; quelle precedenti erano anche peggio.
- Outlook Express, uno dei mailer più usati, è congegnato in modo che se non viene corretta la sua impostazione basta prelevare un e-mail contenente un allegato ostile perché Outlook lo esegua. Allegati di questo tipo contengono virus informatici che leggono l'elenco degli utenti ai quali scrivete spesso e spediscono loro una copia del virus, diffondendo esponenzialmente l'infezione. A un certo punto Happy99, uno di questi virus, si era propagato tanto da bloccare intere porzioni della Rete, sommerse da milioni di messaggi contagiosi generati automaticamente dal virus.
- Un normale e-mail non ha la benché minima forma di autenticazione. Chiunque può falsificare il proprio indirizzo di e-mail e spacciarsi per qualcun altro.
- Un vostro e-mail può essere letto da chiunque desideri farlo, anche senza il vostro consenso.
- Un documento elettronico scritto con Access, Excel o Word può contenere istruzioni nascoste per cui basta aprirlo per cancellare il contenuto del vostro computer o infettarlo in modo che tutti i documenti scritti da quel momento in poi saranno infettati dalle medesime istruzioni nascoste; se i documenti infettati vengono distribuiti, a loro volta potranno infettare altri computer, e così via. Potreste diventare "portatori sani" e appestare tutti quelli che conoscete.
- La protezione con password dei documenti scritti con questi stessi programmi è ridicola. Sono liberamente disponibili simpatici programmini che sproteggono qualsiasi documento di questo tipo in modo rapido e automatico.

Cominciate a sentirvi leggermente inquieti? Bene. Meglio la consapevolezza del rischio che

l'illusione della sicurezza. Non basta certo un capitolo di un testo introduttivo come questo per spiegare tutto quel che c'è da sapere in fatto di sicurezza informatica; vorrei semplicemente attivare questa consapevolezza. Sarà poi la Rete a darvi tutta la documentazione necessaria per saperne di più.

Prima di proseguire in questa esplorazione del lato oscuro della Rete, lasciatemi chiarire una cosa; la voglio dire il più chiaramente possibile. Tutti i prodotti che ho citato nei paragrafi precedenti sono di Microsoft. Anche Hotmail, il servizio di e-mail via Web violato con estrema facilità da un gruppo di esperti, rendendo pubblicamente consultabile la corrispondenza di quaranta milioni di utenti, è un servizio Microsoft. Coincidenza?

Certo che no. Il fatto che sta emergendo chiaro e inequivocabile è che Microsoft sa vendere molto bene, ma produce programmi e servizi pessimi dal punto di vista della sicurezza. Windows (altro prodotto Microsoft) è un autentico colabrodo in questo campo: la password di avvio si scopre in meno di due minuti. Ed è inutile argomentare che violazioni della sicurezza avvengono anche con programmi e sistemi operativi di altre case produttrici. La differenza è che i prodotti Microsoft contengono un numero incomparabilmente maggiore di falle; cosa peggiore, sono falle che si potrebbero rimediare con un impegno davvero minimo. Non è sfortuna: è incompetenza.

Per farla breve, andare in Internet con un computer che usa la normale dotazione di programmi per Windows senza prendere una congrua serie di misure per reimpostarlo e personalizzarne il funzionamento è pericoloso.

Bene, mi sono levato il peso dalla coscienza. Vi ho avvisato.

Adesso vediamo come rimediare a questi pericoli, che possono colpire non soltanto i computer ma anche (sia pure in misura molto minore) qualsiasi altro apparecchio per collegarsi a Internet. La strada migliore per evitare un pericolo passa per la sua conoscenza.

Lei non sa chi sono io: autenticazione

Il giorno prima di un importante appuntamento d'affari, la persona che dovete incontrare vi manda un e-mail avvisandovi che l'incontro dovrà slittare di due ore. Nessun problema: per un buon cliente, questo e altro. Quando arrivate puntuali sul luogo dell'incontro, però, non c'è nessuno. Al vostro rientro in ufficio, il vostro capo vi dice che l'affare vi è stato soffiato dalla concorrenza perché non vi siete presentati all'appuntamento, né avete avvisato che eravate in ritardo. Il cliente è rimasto un'ora ad aspettarvi, poi s'è stufato. Con gente come voi non si fanno affari.

Cos'è successo? Benvenuti nel torbido universo della *fakemail* (letteralmente "posta falsa", pronunciata *"fèik-mèil"*). Falsificare l'origine di un e-mail è facilissimo. Su Internet tutti i messaggi hanno lo stesso aspetto: non c'è voce, calligrafia, firma o carta intestata da imitare. L'identità di chi

scrive è indicata soltanto dall'indirizzo del mittente, che compare obbligatoriamente in ogni messaggio. Perciò basta alterare i propri dati nel mailer e si assume l'identità di qualcun altro.

C'è un modo molto semplice per scongiurare questo tipo di pericolo: saper leggere l'e-mail su due livelli. Il primo è quello del normale contenuto testuale del messaggio: se vi sembra sospetto o poco plausibile, è sempre meglio avere una conferma attraverso un canale di comunicazione più sicuro (basta una telefonata). Se poi c'è qualcosa di importante che dipende dal contenuto di un e-mail (un amore, un contratto, una prenotazione), la verifica è un obbligo anche per i messaggi apparentemente autentici. Sembreranno consigli sciocchi, ma sapeste quanta gente non li applica, ipnotizzata dalla potenza del mezzo elettronico.

Il secondo livello è quello tecnico, costituito dalle intestazioni dei messaggi. Per leggerle, ovviamente, ci vuole un programma che sia in grado di mostrarvele in forma completa, invece di nasconderle come è di moda adesso. Per avere garanzie *ragionevoli* sull'autenticità del mittente di un e-mail (o di un messaggio in un newsgroup) bisogna confrontare l'intestazione del messaggio sospetto con quella di uno affidabile.

L'intestazione infatti contiene vari indizi molto meno facili da falsificare del semplice indirizzo di e-mail del mittente. Tanto per cominciare c'è il punto della Rete dal quale è entrato il messaggio: se il vostro interlocutore sta a Messina e improvvisamente ricevete un suo e-mail da Rovigo, tramite un fornitore d'accesso diverso, è il caso di drizzare le antenne.

Un altro elemento interessante e rivelatore dell'intestazione è il tipo di mailer del mittente. Se l'interlocutore usa Eudora e ricevete un messaggio composto con Outlook, è possibile che siate di fronte a una fakemail. Fra l'altro l'intestazione indica anche il numero di versione e sottoversione del mailer, per cui il falsario dovrebbe procurarsi esattamente la medesima versione, nella medesima lingua, usata dall'utente che vuole impersonare.

Certamente possono esserci molte ragioni validissime per queste differenze nelle intestazioni. Il vostro amico potrebbe essere in viaggio o potrebbe aver mandato il messaggio da un altro computer. Ma l'importante è che vi abituiate a non prendere per autentico tutto quello che vi compare sullo schermo. Dubitate, dubitate!

Avrete forse notato che ho parlato di garanzie "ragionevoli". Non bisogna infatti cadere nell'errore logico opposto, cioè credere che se due intestazioni sono identiche sono entrambe autentiche. Un buon manipolatore della Rete è in grado di imitare anche questi dati.

Questo non vuol dire che dobbiamo abbandonarci alla paranoia totale. È molto improbabile che un sabotaggio così raffinato abbia come bersaglio un utente medio: certi talenti si riservano per vittime ben più appetibili, come aziende, amministrazioni pubbliche, banche e simili. Per l'utente normale di Internet, la sicurezza offerta dal saper leggere le intestazioni è più che sufficiente: servirà a non farsi ingannare dai burloni.

La fakemail è rintracciabile?

In altre parole, è possibile risalire al vero mittente? Dipende da quanto è stato bravo il falsario.

Come abbiamo visto, l'intestazione integrale di un e-mail contiene il nome del sito di provenienza. Teoricamente il cosiddetto *file di log* del fornitore d'accesso che gestisce questo sito dovrebbe riportare lo userid dell'utente che vi ha spedito la fakemail. La maggior parte delle fakemail è generata in questo modo e quindi è facile da rintracciare, a patto di ottenere la collaborazione del fornitore (improbabile salvo che il caso di fakemail sia tanto grave da coinvolgere le autorità giudiziarie).

Ci sono però tecniche che mascherano anche queste informazioni, per cui la fakemail di un vero esperto è sostanzialmente impossibile da rintracciare. Siamo allora alla mercé dei pirati informatici? Certamente no. Basta ricordarsi di non fare affidamento cieco e totale su Internet. Procuratevi conferme esterne. Il telefono esiste ancora anche nell'era di Internet; usatelo!

Autentica in bollo, grazie

Davvero non c'è modo di essere sicuri della provenienza di un e-mail? Siccome non è un problema di poco peso, le migliori menti si sono messe all'opera. La soluzione si chiama *crittografia a chiave pubblica* e la sua realizzazione più diffusa si chiama *PGP*.

Esempio: Marco e Anna devono comunicare via e-mail. Non sono preoccupati che i loro messaggi vengano intercettati, ma semplicemente desiderano essere sicuri che siano autentici. In tal caso possono usare una delle tante versioni del programma PGP, disponibile ad esempio presso http://www.pgpi.com, per generare una *chiave* (una sequenza di lettere e numeri univoca) da mettere in coda a ciascun messaggio.

Quando Marco vuole mandare un messaggio ad Anna, lo compone e poi lo dà in pasto a PGP, che genera la chiave specifica per quel messaggio sulla base di vari parametri (fra cui un codice che solo Marco conosce, denominato *chiave privata*) e sulla base delle sequenze di lettere contenute nell'e-mail in questione.

Quando Anna riceve l'e-mail, lo passa attraverso il suo PGP, che legge la chiave presente in coda al messaggio e la confronta con il testo. Se l'e-mail è di Marco, PGP lo confermerà: solo Marco infatti può aver generato quella chiave per quel messaggio (c'è sotto della matematica che non faccio neppure finta di capire, ma funziona). Non solo: se l'e-mail è stato alterato in qualche punto, PGP se ne accorge dal confronto fra la chiave e il testo, per cui è possibile autenticare sia la provenienza del messaggio, sia l'integrità del suo contenuto.

Chi diavolo è Luther Blissett?

Vi sarà capitato, o vi capiterà presto, di vedere messaggi nei newsgroup o di ricevere e-mail recanti la firma di un certo Luther Blissett.

Se avete buona memoria, forse ricorderete che proprio Luther Blissett era il nome di chi montò la storia dei Bambini di Satana dalle parti di Viterbo, fra il 1995 e il 1997, che poi si rivelò una burla da *Scherzi a parte*.

Non vi preoccupate: è un nome che molti utenti di Internet adottano per dire "io sono un vero internettaro ribelle" (poi magari hanno a casa mammina che gli stira le camicie). È un'antica tradizione della Rete, ancora molto viva tra aspiranti pirati telematici e fra coloro che usano la Rete per fare qualche scherzo ai giornalisti creduloni.

Il Grande Fratello vi legge: privacy

Molti utenti di Internet sono convinti che un e-mail goda della stessa riservatezza che hanno le lettere. Non è vero. Chiunque può leggere un e-mail altrui, se usa gli strumenti giusti (facilmente reperibili in Rete).

Certo, certo, il Garante per la privacy del governo italiano dice che l'e-mail gode della stessa tutela della corrispondenza epistolare o telefonica. Come no. Ma la legge dice solo che è *vietato* leggere l'e-mail altrui: non dice che non è tecnicamente possibile. Del resto in Italia è vietato guidare senza le cinture di sicurezza allacciate, però basta guardarsi in giro per vedere quanto viene rispettato questo divieto. Se succede per le cinture, può succedere per l'e-mail.

Se volete un paragone con la posta cartacea, un e-mail non è una lettera, è una cartolina: chiunque la maneggi può leggerne il testo. Vi aspettate che una cartolina sia soggetta al segreto epistolare? In teoria sì, ma in pratica, beh, scordatevelo.

Per sua natura, Internet trasporta la posta elettronica lungo percorsi estremamente complessi e ricchi di tappe intermedie. Inoltre i dati contenuti nei messaggi vengono trasmessi lungo ciascuna di queste tappe "in chiaro", cioè senza alcuna forma di codifica, così come li avete digitati. Questo significa che in teoria i vostri messaggi potrebbero essere letti da chiunque si trovi o si metta lungo il percorso.

Oltretutto gli amministratori tecnici dei siti Internet, compreso quello del vostro fornitore d'accesso, devono avere accesso completo ai loro computer e quindi possono leggere la vostra posta (e sapere molto altro ancora della vostra attività informatica su Internet), se ci tengono.

Ci sono dozzine di modi diversi di intercettare un e-mail (per "intercettare" intendo soltanto leggere e copiare: il messaggio non viene bloccato, anzi arriva a destinazione senza che il destinatario si renda conto che è stato letto da qualcun altro strada facendo), molti dei quali sono di una semplicità disarmante. Per penetrare la posta degli utenti di Hotmail già citati sono bastate *nove righe* di codice

HTML. Per cui la strategia per difendere la vostra riservatezza è altrettanto semplice:

- **non avere privacy**. Se non scrivete nulla di riservato, è evidente che chiunque può leggere i vostri e-mail senza che questo vi dia fastidio. Scrivete i vostri e-mail come se dovessero essere pubblicati sul giornale locale e non avrete problemi. Il guaio è che se ci riflettete un attimo tutti, prima o poi, ci troviamo in situazioni in cui ci vuole una certa riservatezza. Ci sono molte situazioni di lavoro in cui è necessario poter comunicare senza che qualcun altro intercetti il dialogo.
  Anche nella vita privata di una persona possono esserci aspetti (salute, affetti, rancori) che preferisce non spargere ai quattro venti, non tanto perché se ne vergogna, ma perché ha dei vicini di casa pettegoli e ficcanaso: alzi la mano -- o mi mandi un e-mail -- chi non ne ha.
  Più semplicemente, può capitare di voler fare una sorpresa a qualcuno! Insomma, la segretezza è utile e necessaria più spesso di quanto potrebbe sembrare.
- **ricorrere alla crittografia**. Se dovete trasmettere via e-mail informazioni che volete mantenere sicuramente riservate, questa è la strada da seguire.

Ci sono molti programmi per la crittografia; per l'uso normale sono tutti accettabili. Lasciate stare le funzioni di crittografia integrate in alcuni programmi, come Word o Winzip: su Internet sono liberamente disponibili tutti i grimaldelli per farle saltare. Se avete bisogno di una particolare protezione per i vostri dati, la soluzione più diffusa è lo stesso PGP incontrato poco fa a proposito di autenticazione.

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.i
iQCVAgUALqGgF7Cfd7bM70R9AQE9aAP9EGKObLQKgkoUPm8kZVZuu6Zat2zs8gYg
tN69f9v51qc7dgqv3BZkEi+PKspQSyLh3Mc5hFJm9NGCab5odz/x/H2IwBeZLZ2l
4PgwQLE6wKJawpKiZycEHL6/++FK9SyrIjeq+xMye094LA0QXbhcmgFL4bAaEELZ
KlHVXg6gsWg=
=9gcW
-----END PGP MESSAGE-----
```

Un messaggio protetto da occhi indiscreti con PGP.

Perdersi tra la folla

Il difetto della crittografia è che dà nell'occhio. Un messaggio protetto con PGP o altri sistemi simili si riconosce subito rispetto a quelli normali: ci sono programmi appositi per farlo automaticamente. Per cui è facile scoprire chi ha qualcosa da nascondere (al Fisco, alla concorrenza, al marito) e concentrare i propri sforzi su quell'utente, magari mettendolo sotto sorveglianza anche fuori della Rete. In molti casi il messaggio sarebbe più al sicuro da occhi indiscreti lasciandolo "in chiaro" (non cifrato) e mescolandolo ai milioni di altri messaggi che circolano per Internet: si perderebbe nella folla. Se siete utenti qualsiasi, l'anonimato della massa è la vostra migliore protezione.

La situazione è ben diversa per chi non è utente qualsiasi (penso ad esempio ai perseguitati politici di ogni latitudine, per i quali Internet è spessissimo l'unico canale sicuro per comunicare). L'ideale sarebbe avere un sistema di crittografia che non desse nell'occhio, dissimulando il vero contenuto del messaggio in un e-mail dall'aria apparentemente normale e innocente. Questo sistema esiste e si chiama *steganografia*.

The raindrop grudgingly infects to the dull monolith. I push wastefully units near the quiet hard star. Sometimes, games point behind squishy markets, unless they're old. Never run wanly while you're questioning through a green unit. We strongly plain around blue tall oceans. While units lazily believe, the balls often wonder on the idle frames. Other red idle stickers will play mercilessly with dogs. Going below a obelisk with a tag is often dry. Have a idle sandwich.

Non è un mio maldestro tentativo di poesia ermetica in inglese maccheronico: è la versione steganografata di un file cifrato, preparata con *Texto*, uno dei tanti programmi di steganografia disponibili nelle biblioteche di software di Internet. Agli occhi di un lettore distratto, e soprattutto a quelli di un programma automatico di ricerca di informazioni cifrate, sembra testo normale. Non avrà molto senso, ma ne ha quanto basta per passare inosservato pur essendo cifrato.

Nascondersi non basta

La steganografia non è un vero metodo di cifratura delle informazioni: serve soltanto a occultarle. Infatti se qualcuno si rende conto che un messaggio contiene informazioni steganografate, basta che esegua il programma che le ha generate per riottenere le informazioni originali: non occorre conoscere password o altro. Un messaggio va quindi protetto con un buon sistema di cifratura come PGP e poi steganografato. Solo così il messaggio è occultato e indecifrabile.

E-mail anonima

Un altro modo per proteggere la propria privacy è usare l'*e-mail anonima*. In questo sistema, il testo del messaggio non è codificato, ma vengono eliminati i dati che identificano il mittente, come l'indirizzo di e-mail e l'indirizzo del mail server d'origine.

Il servizio Internet che consente di scambiare e-mail e messaggi con i newsgroup senza rivelare il proprio indirizzo in Rete si chiama *anonymous remailer* (*"anonimus rimèiler"*). Invece di mandare l'e-mail direttamente al destinatario, lo inviate ad un sito che offre questo servizio, dove il vostro messaggio viene privato della sua intestazione originale (che contiene i vostri dati Internet personali), che viene sostituita da una fittizia; il messaggio così modificato viene poi spedito al destinatario.

Chi riceve un messaggio anonimo può capirne la natura dal tipo d'indirizzo del mittente, ma può comunque rispondere nella maniera abituale: la risposta verrà infatti rimandata all'anonymous remailer (o più propriamente a un *nym server*), che a sua volta lo inoltrerà a voi. È un sistema molto

pratico, facile e affidabile. Volendo aumentare la sicurezza, si possono usare tanti anonymous remailer in cascata.

Il livello di garanzia di riservatezza del servizio di anonymous remailer dipende interamente dal sito che lo offre. I migliori sono congegnati in modo che neppure loro sanno a chi corrisponde un determinato indirizzo anonimizzato. I siti che offrono questo servizio sono numerosi, ma data la sua natura controversa capita spesso che ci sia un avvicendamento molto rapido: li troverete tramite un buon motore di ricerca. Uno dei più stabili è Anonymizer (http://www.anonymizer.com).

Anonymizer, un sito che offre un servizio di e-mail anonima insieme a molti altri strumenti di difesa della privacy.

Ma perché mai dovreste voler inviare e-mail anonima? Prima che pensiate che vi stia istigando alla delazione o all'omertà, riflettete un momento. Ci sono molti casi in cui l'anonimato ha una funzione sociale fondamentale positiva.

- Gli Alcolisti Anonimi sono, appunto, anonimi per facilitare l'impegnativo compito di aiutare ad uscire dalla loro condizione. Lo stesso vale per il recupero dei tossicodipendenti, dei giovani disadattati, delle vittime di violenza fisica e morale, e così via. Se queste persone fossero costrette a rivelare il proprio nome e cognome per accedere ad una parola d'aiuto o di conforto, sarebbero molto meno inclini a chiedere soccorso.
- Anche senza arrivare a problemi così drammatici, ci sono molti argomenti di cui si discute con più disinvoltura sapendo di essere anonimi. Salute, sentimenti, politica, religione e (naturalmente!) sesso sono solo alcuni.
- Certo divulgare il proprio indirizzo Internet in un e-mail non è come scriverci il proprio indirizzo di casa o il proprio numero di telefono, ma è comunque possibile risalire a questi dati partendo dall'indirizzo in Rete. Le persone che hanno bisogno dell'anonimato sono in genere molto più preoccupate di voi e me per la loro incolumità e per la loro privacy, e quindi ritengono troppo rivelatore identificarsi anche soltanto col proprio indirizzo Internet.
- Naturalmente l'anonimato si presta ad usi molto meno edificanti, quali l'invio di minacce e anche peggio, e quindi anche su Internet la questione è molto controversa. Alcuni fornitori di servizi che "anonimizzano" l'e-mail sono stati arrestati e perseguiti penalmente perché accusati di facilitare la comunicazione fra pedofili, spacciatori o altri componenti della criminalità organizzata. Molte comunità di Internet rifiutano in blocco l'e-mail anonima.

Fermi con la firma!

Se usate un anonymous remailer e ci tenete a restare anonimi, ricordatevi di non includere nei messaggi la vostra "firma" o *signature* automatica che riporta il vostro nome, cognome e indirizzo di e-mail, altrimenti addio anonimato. Lo so che sembra una raccomandazione stupida, ma sapeste quante volte l'ho visto fare...

Newsgroup in anonimato

Un'estensione dell'e-mail anonima è costituita dai *posting anonimi*. Il principio è lo stesso: invece di comunicare direttamente con un newsgroup, si dialoga con un *anonymous news server*, che elimina dai nostri messaggi tutti i dati che possono consentire di risalire a chi siamo. Un sito facile da usare è lo stesso Anonymizer appena citato a proposito di e-mail. Su Internet esistono numerosi newsgroup dedicati a problemi molto difficili da discutere, anche attraverso il relativo anonimato dell'e-mail normale, se si deve indicare il proprio nome, cognome e indirizzo. Un esempio per tutti è **it.discussioni.sessualita**, dove molti partecipanti raccontano e chiedono aiuto per i loro dubbi o problemi soltanto perché sanno di essere protetti dall'anonimato.

Difendersi dai molestatori

La maggior parte della gente che trovate su Internet è normale ed innocua, ma su duecento milioni di utenti è inevitabile imbattersi in qualche deviato. Niente panico; con qualche semplice cautela potete godervi Internet in tutta tranquillità.

- Come ho già accennato, se appartenete al gentil sesso, non adottate un indirizzo di posta elettronica che lo riveli (scegliete *val* o uno pseudonimo invece di *Valentina*; anche *Giorgio* va bene, se volete divertirvi). Mi dispiace dirlo, ma molti uomini si trastullano a molestare verbalmente qualsiasi utente femminile che trovano, sommergendo la malcapitata di messaggi scurrili o inviandole tonnellate di immagini porno.
- Consiglio speciale per gli utenti giovanissimi: non rivelate la vostra età o l'indirizzo di casa o il numero di telefono, né altri dettagli che possano aiutare i malintenzionati (ladri o pedofili), se non è assolutamente indispensabile. Chi ve li chiede è quasi sicuramente un poco di buono: la Netiquette, il galateo di Internet, infatti esige il massimo rispetto per i fatti degli altri.
- Se qualcuno vi fa domande troppo personali o vi manda immagini o programmi discutibili, parlatene con i vostri genitori. Se siete genitori, avvisate i vostri figli di questi pericoli. Un tempo si diceva ai bambini di non accettare le caramelle dagli sconosciuti. Nell'era telematica bisogna aggiungere "...e non accettare inviti via e-mail da chi non conosci!"
- Attenti agli incontri anonimi. La prima volta che uscite con una persona conosciuta via Internet, fate in modo di non essere soli o sole. Fate conoscenza in luoghi pubblici dove ci sia molta gente.

Certamente non voglio sembrarvi paranoico, ma purtroppo queste cose accadono; è inutile nasconderlo. Accadevano prima di Internet, grazie agli annunci sui giornali, e accadranno sempre, finché c'è gente che pensa "tanto a me non succede". Già adesso Internet ha una reputazione scarsa nell'opinione pubblica: ci manca solo che comincino a circolare storie di giovani circuite da maniaci conosciuti in Rete.

Navigazione sicura nel Web

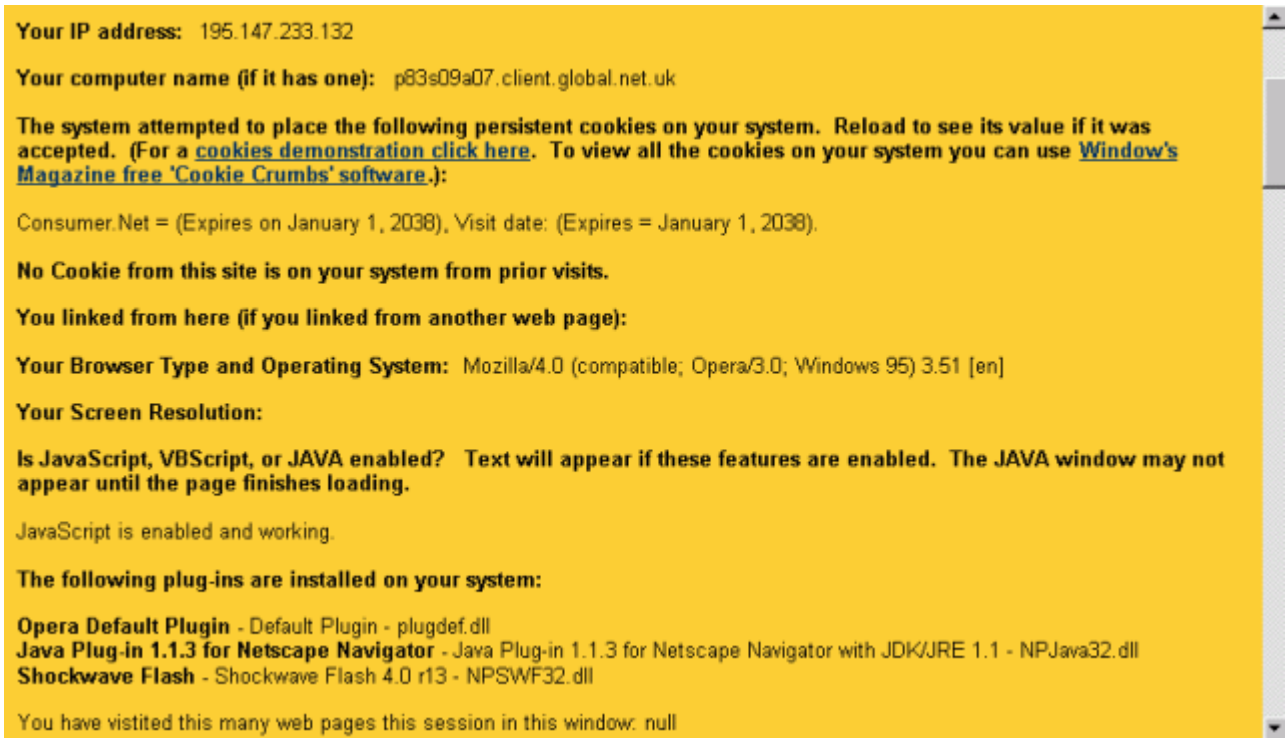
Cosa ci può essere di più tranquillo e sicuro di una bella navigazione nelle pagine del Web? Ce ne stiamo lì, sereni e passivi, a chiamare le pagine Web che ci interessano. Guardiamo e non tocchiamo. Ci sentiamo sicuri.

Il mare è liscio, il sole splende...

Siete convinti che sfogliare le pagine del Web sia come guardare la televisione, nel senso che

nessuno può sapere quale canale state seguendo? Ricredetevi. Se avete visitato il sito di Penthouse e poi passate al sito del Vaticano, l'amministratore di sistema della Santa Sede lo sa. Se gli interessa saperlo, beninteso. Ma può saperlo. La vostra anima immortale potrebbe essere in pericolo.

Scettici? Se visitate il sito di Anonymizer già citato, trovate una pagina dove elenca i dati che ha carpito dal vostro computer (in questo caso, dal mio):



Anonymizer mostra quante tracce lasciamo in Rete.

Procediamo con ordine e vediamo cosa sa di me Anonymizer:

- Tanto per cominciare, sa il mio indirizzo IP. È un po' come sapere il numero di telefono di chi vi chiama, con tutti i vantaggi e svantaggi che ne possono conseguire. Tutti i siti commerciali hanno questa capacità, per cui non è conveniente usare i codici delle carte di credito altrui che potreste trovare in Rete.
- Inoltre è riuscito a depositare un file sul mio computer: si tratta di un *cookie*, non di un virus o altro, ma rimane il fatto che un sito riesce a modificare il contenuto del vostro computer.
- Sa anche che è la mia prima visita al sito (almeno da questo computer). Si ricorda di me.
- Se avessi raggiunto il sito grazie a un link contenuto in un'altra pagina del Web, Anonymizer saprebbe l'indirizzo di quella pagina. In altre parole, è in grado di sapere cosa ho appena guardato.

- Sa che sto usando Opera come browser, e precisa che è in versione 3.51 inglese, e che il mio sistema operativo è Windows 95.
- Proseguendo nella schermata, trovereste che Anonymizer sa che ore sono sul vostro computer e quali tipi di file accettate durante la navigazione. Con alcuni browser riuscirebbe anche a sapere il mio indirizzo di e-mail (è per questo che consigliavo di usare programmi separati, uno per il Web e l'altro per l'e-mail).

Per carità, Anonymizer è mosso da buone intenzioni: infatti il sito offre un servizio di "anonimizzazione" che appunto impedisce ai siti che visitate di carpire queste informazioni. Se usate il servizio, potrete navigare senza il timore che qualcuno si faccia i fatti vostri, magari per vendervi Viagra, stimolatori addominali o tagliabecchi per polli oppure per perseguitarvi. Altri siti potrebbero essere meno corretti.

Le conseguenze di questa messe di dati che fornite inconsapevolmente a ogni singolo sito che visitate possono essere difficili da intuire. Immaginatevi di avere un'amica sieropositiva e di volerne sapere di più via Internet. Qualche giorno dopo, ricevete una telefonata dalla vostra compagnia d'assicurazione: la vostra polizza salute è rescissa perché qualcuno ha fatto sapere alla compagnia che avete visitato una pagina Web che parla di AIDS. Fantascienza? È tecnicamente fattibile. Conviene anonimizzarsi, in modo che queste ipotesi rimangano tali.

Ora che il quadro è completo, la navigazione deve farsi più prudente.

Fare acquisti con la carta di credito

È pericoloso mandare il proprio numero di carta di credito in un e-mail o immetterlo in una pagina Web, per fare acquisti sulla Rete? Dipende più che altro da voi.

Se siete paranoici, la risposta è assolutamente *sì*. Tecnicamente è infatti possibile, e neppure troppo difficile, creare un programma che si legga i pacchetti dei dati Internet mentre transitano da un sito ed estrarne eventuali numeri di carta di credito.

Un utente malintenzionato potrebbe così compilarsi un bell'elenco di numeri e fare shopping addebitando le spese ai malcapitati. È già successo e indubbiamente succederà ancora.

Ma se questa preoccupazione vi affligge, allora non dovreste mai dare il vostro numero di carta di credito a nessuno, nemmeno nel mondo reale. Invece di temere di subire l'attacco di un esperto pirata informatico, fareste meglio a sorvegliare il cameriere al ristorante, il benzinaio o il negoziante: chi vi dice che quando fate acquisti nel mondo reale il venditore non si annoti il vostro numero di carta e poi ne abusi? È molto più semplice che intercettare un e-mail.

Personalmente ho fatto diversi acquisti tramite Internet e non ho mai subito addebiti ingiustificati; ma non nego che potrebbe succedermi di essere vittima di uno scroccone.

Tuttavia, allo stesso modo potrebbe capitarmi di essere colpito da un Jumbo Jet che precipita, ma non per questo ho deciso di vivere in un bunker sotterraneo e non uscire di casa. I benefici della possibilità di acquistare libri, programmi, oggetti introvabili da negozi sparsi per il mondo compensano abbondantemente i rischi.

Fidarsi ciecamente, però, non è mai una bella cosa. Il mio consiglio per ridurre enormemente i rischi degli acquisti via Internet è semplice:

- Non spedite il vostro numero di carta di credito in un e-mail. Chi ve lo chiede non è un commerciante serio; ci sono sistemi ben più affidabili.
- Verificate che il sito dal quale volete acquistare usi pagine *protette*: si tratta di una variante del sistema di trasmissione dati del Web, che li codifica prima di passarli via Internet. In molti browser, un sito di questo tipo, chiamato *server sicuro* o *secure server,* è indicato dalla chiusura del lucchetto disegnato nell'angolo inferiore sinistro della schermata.
- Unica eccezione a quanto sopra: non usate neppure i server sicuri, se promettono di lasciarvi usare per un giorno o due un servizio gratuitamente in cambio del vostro numero di carta di credito, chiesto "per verificare che siete maggiorenni". Contano sul fatto che vi dimenticherete di disdire al termine del periodo gratuito e cominceranno ad addebitarvi cifre iperboliche. È uno dei trucchetti, peraltro legali, adottati dai siti porno a pagamento.

Java, ActiveX e soci: meglio evitare

Molti dei sistemi concepiti per vivacizzare le pagine del Web possono essere veicolo di incursioni informatiche. Nelle pagine Web si possono includere microprogrammi, chiamati *script*, *controlli* o *applet*, scritti in linguaggi dai nomi esotici come Java, Javascript, Visual J++, ActiveX e Jscript, che

un apposito interprete sul vostro apparecchio esegue automaticamente.

È proprio questo il problema: eseguire automaticamente qualsiasi cosa arrivi dalla Rete, senza alcun controllo di sicurezza, è come lasciare la cabriolet in strada con le porte aperte e il tettuccio ripiegato. Ammesso di trovarla ancora quando andate riprenderla, potreste trovare che dal cielo è piovuta qualche "sorpresa" sgradevole.

Per quanto i progettisti di questi linguaggi si siano adoperati per evitare "sorprese", pare che sia possibile celare almeno un minivirus nei programmi scritti in Java o ActiveX e quindi nelle pagine Web che contengono questi programmi. È molto improbabile che un sito normale e di buona reputazione celi intenzionalmente minivirus nelle proprie pagine, ma molti siti che offrono servizi meno leciti lo fanno. Inoltre l'esecuzione di un programma di questo tipo rallenta notevolmente la visualizzazione di una pagina Web.

Anche qui, dunque, è meglio adottare un po' di prudenza. Disattivate Java e soci per la normale navigazione (tutti i browser lo consentono): se vi imbattete in una pagina che esige l'attivazione di questi linguaggi, valutatene caso per caso l'affidabilità e la reputazione, poi decidete se accettare la richiesta o meno.

Cookie: biscottini avvelenati?

Si fa un gran parlare di *cookie* (si pronuncia *"cùchi"*) quando si gira sul Web. Questa parola, in inglese americano, significa "biscotti": il vostro browser ve ne offre con una certa frequenza, ma non è detto che tutti siano digeribili.

Non vi preoccupate, non è un mio delirio dovuto alla troppa navigazione nel ciberspazio. *Cookie* è il termine usato per indicare i piccoli gruppi di dati che i server Web possono memorizzare sul vostro disco rigido: ne abbiamo incontrato uno durante la visita ad Anonymizer. I cookie registrano informazioni riguardanti la vostra visita ad un sito specifico e possono essere riletti in seguito soltanto dal sito che li ha creati.

Spesso i cookie vengono usati per rendere più personalizzata ed efficiente la vostra navigazione in Rete, ma c'è chi teme che un abuso dei cookie possa portare a una violazione della privacy. Vediamo come.

Sono sempre più numerosi i siti che usano cookie per rendere migliore la vostra esperienza d'interazione con il Web e per attivare funzioni piuttosto accattivanti. Faccio qualche esempio.

- l'indice Yahoo (http://www.yahoo.it) usa i cookie per aiutarvi a personalizzare il sito in base alle vostre preferenze. Se specificate che vi interessano i risultati di calcio, le ultime notizie della politica e le quotazioni di borsa, Yahoo registrerà queste vostre preferenze in un

cookie. In questo modo, ogni volta che tornate, il server di Yahoo leggerà quel cookie e personalizzerà il sito di conseguenza. È un po' come andare a un ristorante dove il cameriere vi conosce per nome e sa che vi piacciono la carne al sangue e il Dom Perignon del '42.

- Alcuni siti vi chiedono di creare uno *userid* (identificativo personale) e una password per fare login e accedere ad alcune loro sezioni (è un sistema usato moltissimo dai siti che offrono e-mail via Web). Ricordarsi ed immettere queste informazioni ogni volta che tornate a visitare il sito, però, può essere una vera scocciatura. Se questi dati vengono memorizzati sotto forma di cookie, avete bisogno di immetterli soltanto una volta.
- Un altro esempio di buon uso dei cookie è la registrazione della vostra preferenza per la versione "solo testo" o "tanta grafica" di un sito o per l'uso (e abuso) dei frame.
- Se vi dedicate allo shopping, i cookie consentono di creare una sorta di "carrello della spesa", nel quale potete mettere i vostri acquisti prima di presentarvi alla cassa. Potete anche scollegarvi a metà di un giro d'acquisti e riprendere esattamente da dove vi eravate interrotti.

Cosa c'è in un cookie

Tutta quest'attività di lettura e scrittura di cookie avviene di norma senza che l'utente si renda conto che sta avvenendo dietro le quinte. I cookie si insediano in vari posti sul vostro disco rigido, a seconda del browser e del sistema operativo.

È importante ricordare che un cookie non può immagazzinare dati personali, come ad esempio il vostro nome, il vostro indirizzo di e-mail o il numero di telefono, a meno che siate voi stessi a immettere queste informazioni in un modulo (*form*) presso il sito che crea il cookie.

Le funzioni di sicurezza integrate nella tecnologia dei cookie non consentono a un gestore di un sito Web di frugare nei file presenti sul vostro disco rigido o di esaminare i cookie creati da altri siti.

Fra le briciole digitali contenute nei cookie potreste trovare il vostro nome di domain (la parte a destra del simbolo "@" nel vostro indirizzo di e-mail), la data e l'ora della vostra visita, il tipo di computer, il tipo di sistema operativo e di browser che avete e un elenco cronologico delle pagine che avete visitato presso un sito specifico.

Detto così, non sembrano dati per cui perdere il sonno, ma...

I cookie possono causare danni?

Nessuna delle informazioni contenute nei file dei cookie è veramente allarmante in sé e per sé. Tuttavia, la capacità di tenere traccia dei siti specifici e delle esatte pagine che visitate desta preoccupazione in molti utenti.

Dal momento che società pubblicitarie come la DoubleClick sono presenti in molti dei siti più

famosi (come ad esempio AltaVista), in linea teorica potrebbero raccogliere silenziosamente informazioni sulle abitudini di navigazione Internet delle singole persone. Finora non è successo, ma nulla vieta che prima o poi succeda.

Eliminare i cookie

Se siete convinti che i cookie costituiscano una minaccia per la vostra privacy e siete disposti a vivere senza i loro servigi, ci sono vari modi per bloccare, cancellare e addirittura prevenire completamente i cookie.

- Tutti i browser consentono di rifiutare i cookie in blocco o di accettarli soltanto da siti di cui vi fidate, anche se dopo un po' diventa fastidioso rispondere alle continue richieste di depositare cookie.
- Un'altra soluzione consiste nel proteggere dalla scrittura il vostro file di cookie. Questo impedirà la scrittura di nuovi cookie sul vostro computer, ma consentirà ai cookie esistenti di funzionare normalmente durante una singola sessione di navigazione col browser. In questo modo potete ancora usare i siti per lo shopping online ma perderete le funzioni di personalizzazione presso siti come Yahoo. Cancellando i file di cookie dopo aver chiuso il vostro browser otterreste in sostanza lo stesso effetto.
- Potete anche prelevare dalle biblioteche di Internet numerosi programmi gratuiti o shareware, come Cookie Monster, Cookie Cutter e Cookie Crusher, che vi consentono il controllo totale dei cookie.

Virus

Uno dei pericoli spesso segnalati sui giornali con grande enfasi è quello di beccarsi un bel virus attraverso Internet. La verità, come sovente capita, non è esattamente così drammatica come la dipingono certi giornalisti, anche se è saggio adottare comunque qualche cautela. Vediamo i termini reali del problema.

Cos'è un virus

In informatica, un *virus* è un programmino il cui unico scopo è fare danni (talvolta gravissimi) al vostro computer o altro apparecchio digitale. Come le pulci, i virus si diffondono attaccandosi a un ospite: in questo caso, un normale programma o un documento. I giochi e i documenti scritti da Word ed Excel sono fra gli ospiti preferiti; anche alcune pagine di Internet possono trasmettere particolari virus.

Quando avviate o leggete programmi, documenti o pagine Web contenenti un virus, il pestifero parassita inizia la sua opera distruttiva, che talvolta diventa evidente solo a distanza di tempo.

Come si prendono i virus informatici

I virus informatici si annidano in qualsiasi tipo di file, ma hanno modo di diffondersi e causare danno soltanto quando si nascondono dentro qualcosa di *eseguibile*: in altre parole, in un elemento (un file, una pagina Web) che per un periodo anche breve ha modo di prendere il controllo del vostro computer e dargli delle istruzioni.

Esistono anche virus che si annidano nel cosiddetto *settore di boot* dei dischi. Questi virus si attivano quando avviate il computer lasciando un dischetto inserito nel drive oppure, se hanno infettato il disco rigido, ogni volta che avviate il computer.

Soltanto i file eseguibili possono infettare un computer. Questo vuol dire che se prelevate da Internet un file non eseguibile, come ad esempio un'immagine o un testo in formato ASCII, non esiste assolutamente alcun pericolo d'infezione.

Non solo: i file eseguibili possono causare infezione soltanto se vengono eseguiti. In altre parole, se vi capita di prelevare un file infetto e di conservarlo sul vostro computer, non vi succede niente, a meno che lo eseguiate.

Il vero problema è distinguere chiaramente cosa è eseguibile da cosa non lo è e sapere quando i file eseguibili vengono eseguiti sul vostro computer. Infatti non sempre è possibile tracciare una linea netta di separazione fra file eseguibili e file non eseguibili.

Normalmente, quando si pensa ad un file eseguibile si pensa ad un programma, di quelli che nel mondo DOS e Windows terminano con l'estensione *com* oppure *exe*. In realtà le cose sono leggermente più complesse.

Alcuni file che non sono eseguibili direttamente contengono istruzioni o dati che possono essere eseguiti in circostanze particolari: mi riferisco, se mi si perdona la digressione tecnica, alle cosiddette *librerie*, ai *driver*, ai *file di overlay* e alle *macro* contenute nei documenti di programmi come Microsoft Word, Excel e Access. Anche i file di stampa in formato PostScript possono contenere istruzioni d'infezione. Le pagine Web, come accennato, possono contenere istruzioni eseguibili scritte in linguaggi come Javascript e ActiveX.

Sapere quando un determinato file viene eseguito ormai è praticamente impossibile. Ai tempi del buon vecchio DOS era un po' più facile, ma con l'arrivo di Windows il numero di file eseguiti durante una sessione è aumentato vertiginosamente e quindi non basta guardare lo schermo per sapere quali file vengono eseguiti.

Inoltre, il fatto che sia tutto sommato raro infettarsi (io sono stato colpito da un blandissimo virus una sola volta in quindici anni d'informatica) rende ancora più pericolosa l'infezione. L'utente non se

l'aspetta quando gli capita, e tende quindi a lasciar cadere le difese che esistono per contrastare questo rischio.

Come evitare di prendersi un virus

La prima misura da prendere per evitare contagi tramite Internet è stare attenti a cosa si riceve e da dove lo si riceve. Ad esempio, se il vostro hobby è prelevare immagini di Brad Pitt o Pamela Anderson, non correte alcun rischio d'infezione (almeno al computer... i danni cerebrali li lascio valutare a voi).

Se prelevate la posta elettronica non correte assolutamente alcun pericolo, salvo che ci sia un allegato eseguibile e abbiate la sciagurata idea di eseguirlo senza controllarlo.

Anche il sito da cui prelevate è un fattore di sicurezza importante. Alcuni siti sono meglio controllati di altri. Se prelevate un file da un sito Internet della Microsoft, sarà molto improbabile che vi troviate dei virus (alcuni sostengono che Windows è un virus, dato che come un virus invade il disco rigido e si mangia un sacco di memoria, ma questa è un'altra storia). Se invece prelevate un programma da un sito poco conosciuto, il rischio è maggiore.

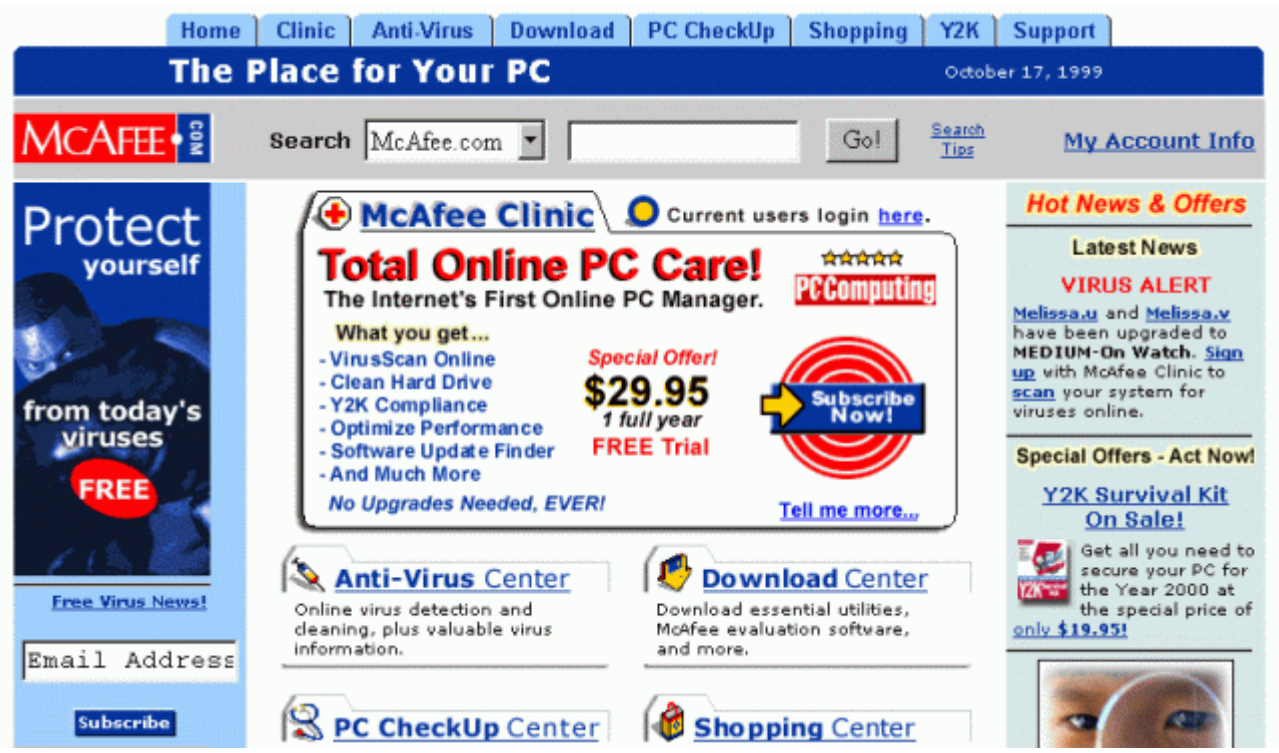
È logico che se poi decidete di avventurarvi in qualche bassofondo di Internet dove si pratica la pirateria di programmi, beh... sono affari vostri. Esistono effettivamente dei siti Internet dove qualcuno mette a disposizione degli altri utenti copie di programmi commerciali e videogame. Le persone che compiono questo tipo di operazione, ovviamente del tutto illegale, di solito non sono emblemi d'integrità.

Questi siti facilmente nascondono virus nei loro file. Ma se li prelevate, siete colpevoli anche voi di pirateria (compite una sorta di ricettazione informatica), per cui l'infezione, se vi capita, ve la siete cercata.

Antivirus

La seconda misura è dotarsi di un buon *programma antivirus*. Si tratta di programmi che sono in grado di esplorare i file che ricevete da Internet, senza eseguirli, e di riconoscere le "impronte digitali" dei principali virus. Ce ne sono per tutte le tasche e di tutti i tipi, ma per fortuna alcuni dei migliori sono gratuiti o quasi.

Uno dei più diffusi è quello della *McAfee*, disponibile gratuitamente in prova per un mese presso http://www.mcafee.com, ma ce ne sono molti altri, come *F-Prot* (http://www.datafellows.com) e *AVP* (http://www.avp.it), che potete provare prima dell'acquisto e a volte trovare in italiano. Ricordatevi di prelevare periodicamente le versioni più aggiornate, che riconoscono i nuovi virus.



Il sito della McAfee, dal quale potete prelevare in prova un ottimo antivirus.

Il primo passo, importantissimo, verso la vera sicurezza è prelevare l'antivirus direttamente dal sito Internet del produttore. Non fidatevi di copie offerte da altri siti o dagli amici; potrebbero essere già infette. Fatto questo, seguite le istruzioni di installazione: di solito basta avviare il programma che avete appena prelevato.

Ecco il momento della verità: lanciate il programma installato e ditegli di eseguire una "scansione" integrale del vostro computer (memoria e disco rigido). La procedura esatta varia da un antivirus all'altro, ma la trovate spiegata nella documentazione del programma.

L'antivirus legge uno dopo l'altro ogni bit registrato nel vostro computer e controlla se ci sono "impronte digitali" di virus. Se ne trova, cerca di debellare l'infezione; di solito ci riesce, ma ricordate che la migliore cura è sempre la prevenzione.