Versione 1.18 – 26 ottobre 2004

[Testo della quarta di copertina:]

Ci credereste che bastano
dodici semplici regole per salvarvi
da tutti gli attacchi informatici
degli ultimi anni?

Sono in questo libro.

Provatele. Gli altri si pentiranno di non averlo fatto.

Capitolo 0
Note per l'edizione digitale

***L'Acchiappavirus* non è protetto in alcun modo contro la duplicazione.** Lo offro alla comunità di Internet senza restrizioni, eccetto quelle imposte dalla vostra onestà. Potete distribuirlo e duplicarlo liberamente, per esempio mettendolo sul vostro sito o facendolo circolare nei circuiti *peer-to-peer*, a condizione che:

- il file rimanga intatto
- non lo facciate pagare (a parte il costo dell'eventuale supporto informatico)
- non ne distribuiate copie stampate (l'esclusiva per l'edizione cartacea spetta all'editore Apogeo)

Il fatto di essere liberamente distribuibile **non altera né indebolisce in alcun modo il diritto d'autore** (*copyright*), che rimane mio, ai sensi delle leggi vigenti.

Il testo originale, integrale e aggiornato di questo libro è disponibile presso ***www.attivissimo.net.***

Se questo libro elettronico vi piace, non mi offendo se andate in libreria e ne comperate una copia su carta, magari da regalare agli amici informaticamente imbranati che vi assillano con continue richieste di aiuto.

Capitolo 1
"Questo libro non mi serve..."

So benissimo cosa state pensando.

State pensando che questo libro non fa per voi per una delle solite ragioni:

- *"Che palle, un libro sulla sicurezza informatica...."*
- *"Tanto io di queste cose non ci capisco nulla"*
- *"Ma io non ho segreti da difendere"*
- *"Ma chi vuoi che ce l'abbia con me"*
- *"Ho l'ultimo Windows, sono invulnerabile"*

Sbagliato. È vero che molti libri di sicurezza sono pallosi (questo no, ve lo prometto), ma tutte le altre giustificazioni sono beate illusioni.

La sicurezza informatica non è difficile: richiede soltanto un po' di buon senso e di conoscenza del mezzo. I virus e gli altri attacchi informatici sparano nel mucchio, non selezionano le proprie vittime, per cui siamo tutti a rischio. Quasi tutti i programmi per computer, Windows compreso, sono dei colabrodo: se non chiudete il libro, ve lo dimostrerò. Sapevate, per esempio, che **con Windows XP non aggiornato può bastare collegarsi a Internet, visitare un sito o soltanto visualizzare un'immagine per infettare il computer?**

Ogni volta che c'è un attacco di un virus, milioni di utenti vengono infettati. Come mai? Forse non è possibile difendersi e questi disastri fanno parte dell'ordine cosmico delle cose? No, perché gli addetti ai lavori sanno benissimo come difendersi. Probabilmente perché hanno letto una catasta di libri pallosi sull'argomento.

Beh, l'ho fatto anch'io, e ho distillato quella catasta in una guida che mi auguro sia digeribile anche per i non addetti ai lavori, che sono poi i più bisognosi di sicurezza, perché sono gli utenti più vulnerabili della Rete.

State pensando che **tanto non avete segreti da difendere?** Allora chiedetevi se vi piacerebbe che qualcuno leggesse la vostra po-

sta o vi spiasse in casa tramite la telecamerina del computer (si può, si può).

Anche se per ipotesi non avete segreti custoditi nel computer, pensate al danno che può farvi un singolo virus che vi distrugge la collezione di musica e di foto memorizzata nel computer, vi blocca l'uso del computer sul posto di lavoro, o fa comparire a sorpresa immagini porno davanti ai vostri figli.

Come funziona questo libro

Si apre la copertina, si legge la prima pagina, si volta la pagina e si legge la seconda, e così via. Visto? I libri di sicurezza informatica non sono poi così difficili.

Battute a parte, non farò grandi ragionamenti teorici. Questo è un libro **pratico**. Di conseguenza, spesso non spiegherò a fondo perché certe misure di sicurezza funzionano: l'importante è che funzionino. Se poi volete approfondire, a vostra disposizione c'è tutta la documentazione presente su Internet (quella pallosa).

I problemi saranno descritti ricorrendo anche a esempi di situazioni reali e a paragoni con problemi analoghi del mondo reale, dando (ove possibile) una cosa che troppo spesso manca in libri come questo: non soltanto la soluzione, ma anche il modo di **verificare** i rimedi proposti.

Quale Windows?

Questo libro è pensato per chi usa Windows, in particolare la sua versione più recente e diffusa, chiamata ***Windows XP Home o Professional,*** in configurazione monoutente, con tutti gli aggiornamenti eccetto quello noto come *Service Pack 2*. Questa è la configurazione più diffusa di Windows XP al momento in cui scrivo. Le correzioni e variazioni introdotte dal Service Pack 2 vengono presentate a parte in ciascun capitolo.

Purtroppo esigenze di lunghezza mi impediscono di coprire in dettaglio anche le installazioni multiutente e i vecchi Windows (95, 98, ME, NT, 2000), che pure sono ancora molto diffusi. Molti dei consigli descritti, comunque, valgono (con qualche ritocco) anche per queste vecchie versioni di Windows.

Per sapere quale versione di Windows XP avete e se avete già il Service Pack 1 e 2, scegliete Start > Impostazioni > Pannello di controllo > Sistema *e cliccate sulla scheda* Generale.

Usate Linux o Mac? Andate via!

Se usate prodotti alternativi, come Linux o Macintosh, fate parte di quella felice élite di persone che non ha così tanti problemi informatici quanti ne abbiamo noi utenti di Windows. Smettetela di gongolare dall'alto della vostra (ahimè meritata) superiorità e andate a compiacervi altrove. Qui c'è gente che soffre, abbiate rispetto.

Alcuni di voi mi conoscono forse per un altro libro che ho scritto, Da Windows a Linux*, e si aspettano quindi che io sia un Linuxiano duro e puro. Non esattamente: più pragmaticamente, ho un computer Mac, uno Windows e uno Linux, e uso il sistema operativo più adatto a seconda dei casi. Qualche volta (non molto spesso) il più adatto è Windows. Non c'è nulla di cui scandalizzarsi.*

Patti chiari, amicizia lunga

Questo libro non ha la pretesa irrealistica di rendervi invulnerabili o di coprire **tutti** i pericoli della Rete: garantisco però che spiega come difendersi dal 99% degli attacchi informatici più diffusi.

Sia ben chiaro, però, che c'è ben poco che possa fermare un intruso molto deciso che ce l'abbia *specificamente* con voi: per difendersi da queste cose ci vuole un esperto di sicurezza informatica che esamini il vostro caso personale. Ma la stragrande maggioranza degli attacchi non è mirata a una persona specifica. ***L'Acchiappavirus*** **vi mostra come proteggervi da queste incursioni casuali.**

Prometto che **non ci saranno paroloni tecnici**. Beh, no, ce ne sarà qualcuno, ma saranno ridotti al minimo indispensabile, tenuti al guinzaglio e comunque riepilogati in un glossarietto in coda al libro. Anzi, ce ne sono due o tre che è meglio chiarire subito, così non ci pensiamo più.

- ***Virus* o *worm*?** Questo è un libro divulgativo. Gli esperti pignoli mi perdoneranno se per semplificare la vita al lettore userò il termine *virus*[1] per indicare sia i virus veri e propri (quelli che si propagano attaccandosi ai programmi e si riproducono quando i programmi infetti vengono eseguiti), sia i programmi che si propagano da soli in una rete di computer, che più propriamente sarebbero da chiamare *worm*[2], ma che nel parlare comune vengono chiamati comunque *virus*. Piuttosto che barricarmi nella pignoleria, preferisco arrendermi alla consuetudine per ovvie ragioni di comprensibilità.

- **Hacker? Non nominateli!** Il guaio della parola *hacker* è che i giornalisti l'hanno abusata e ne hanno storpiato completamente il significato. **Fra gli informatici, *hacker* non è necessariamente un termine negativo:** soprattutto per quelli della vecchia scuola, è un titolo di merito. Un *hacker*, in questa comunità, è chiunque si destreggi con una tecnologia e ne tiri fuori prestazioni non previste dal produttore o normalmente inaccessibili all'utente. Se componete un SMS senza spedirlo e lo usate come improvvisato "blocco note" del telefonino, o usate il codice di comunicazione degli squillini, non previsto dagli operatori telefonici, siete *hacker*: state estendendo *in modo innocuo* le prestazioni della tecnologia. Il termine italiano equivalente è *smanettone*.

  I giornalisti, invece, sempre affamati di parole esotiche da usare come grucce per i loro articoli, si sono appoggiati subito a *hacker*, interpretandolo come sinonimo di *pirata informatico*. Questo ha ovviamente creato moltissima confusione, perché non si è mai sicuri di essere capiti quando si usa questo termine; e ora anche le nuove leve degli informatici stanno prendendo a usare *hacker* in questo senso negativo (il termine inglese corretto sarebbe semmai *cracker*).

  Di conseguenza, in questo libro non troverete mai, d'ora in poi, la parola *hacker*: i "cattivi" saranno sempre chiamati *vandali*, *intrusi* o *aggressori*, e i buoni saranno italianissimi *smanettoni*.

- **E-mail: maschile o femminile?** In questo testo, *e-mail* segue i suggerimenti dell'Accademia della Crusca: maschile se si riferisce al singolo messaggio, femminile se indica il concetto astratto di corrispondenza elettronica. Pertanto io invio *un* e-mail a un amico, ma capita che *la* e-mail di tutti subisca ritardi quando c'è tanto traffico in Rete. Lo so, brutta regola, ma non l'ho inventata io.

Aggiornamenti di Windows: il Service Pack 2

A settembre 2004 Microsoft ha reso disponibile un massiccio aggiornamento di Windows XP, denominato *Service Pack 2*, concepito per dare al sistema operativo Microsoft un *lifting* in termini di sicurezza.

Il prezzo di questi cambiamenti non è modico: per esempio, **numerosi programmi di Microsoft e di altri produttori diventano inservibili.**[3] Il Windows "rinnovato" è infatti molto meno tollerante verso i difetti e le funzioni dei programmi che possono comportare rischi di sicurezza.

È quindi necessario procurarsi versioni più aggiornate dei programmi resi "incompatibili": purtroppo questo è a volte impossibile, per esempio nel caso di software scritto da società non più esistenti o addirittura scritto su misura. Bisogna allora scegliere fra rinunciare ad alcuni programmi e aumentare la sicurezza, oppure conservare la disponibilità dei vecchi programmi e trovare soluzioni alternative per rendere Windows meno vulnerabile.

Una di queste soluzioni alternative è usare la guida che state leggendo per ottenere buona parte dei risultati del Service Pack 2 senza doverlo adottare, salvaguardando così l'investimento fatto nei programmi "vecchi".

Ogni capitolo di questo libro è pertanto scritto partendo dal presupposto che **non** abbiate installato il Service Pack 2, ma include un'apposita sottosezione che descrive le modifiche introdotte da questo controverso aggiornamento di Windows XP.

Aziende, non barate!

Un'ultima cosa. Ho scritto questo libro **per l'utente Windows XP ordinario**, che si collega a Internet tramite un modem o una linea ADSL e ha uno o due computer in casa.

Non ho preso in considerazione le situazioni aziendali (anche se molti dei consigli citati valgono anche in quel contesto) per la semplice ragione che qualsiasi azienda degna di questo nome dovrebbe avere un responsabile per la sicurezza informatica, che se non è un incompetente non ha bisogno di questo libro. Un'azienda, inoltre, dovrebbe dotarsi di politiche di sicurezza basate su apparecchiature e programmi ben al di là della portata economica di un utente privato.

Al massimo, questo libro può essere utile per **dare ai dipendenti un'infarinatura di sicurezza informatica**, ma non deve essere l'unica base della sicurezza aziendale. Qualsiasi organizzazione che basi la propria sicurezza esclusivamente su una guida introduttiva come questa è, per dirla in modo educato, stupidamente incosciente. Tuttavia, se mi passate la squallida autopromozione, può redimersi comperando una copia di questo libro per ogni dipendente.

Due parole per i veri esperti di sicurezza informatica

Non odiatemi.

So benissimo che inorridirete leggendo questo libro e che conoscete mille modi per aggirare tutte le difese che descrivo. Ma non è questo il punto: non ho l'ambizione di scrivere la madre di tutte le guide alla sicurezza informatica. Qui si tratta semplicemente di creare **un libro usabile da chi più ne ha bisogno**, ossia l'utente poco esperto, e che gli consenta di rendere il proprio computer non proprio *invulnerabile* (ammesso che si possa), ma un po' *meno colabrodo*.

Le tecniche descritte qui sono insomma un *"molto meglio di niente"*, frutto di un compromesso fra facilità d'uso e robustezza. È chiaro che si potrebbe fare di più; ma quel "di più" rischierebbe di essere talmente complicato da non essere applicabile in pratica e quindi tutti i bei discorsi finirebbero al vento.

Ringraziamenti

Questo libro non esisterebbe senza il contributo attento e generoso di chi l'ha sostenuto e pazientemente riveduto durante la sua gestazione. *L'Acchiappavirus* è stato pubblicato su Internet già durante la lavorazione, in modo che chiunque potesse sfogliarlo in anteprima e aiutare a snidarne refusi, ambiguità ed errori tecnici. Quelli che restano sono esclusivamente colpa mia.

Un sentitissimo *grazie*, quindi, a:

- **Nickname:** 2geez, bbrunod, BettyBoop, carlocatal, Ce, Darione, darussol, db_61, duende, francesco.fo**i, Franto, gergio, grazianid, joross, Infinity, liuska3, luca, Luca "er bimbo", lucajdvr, manhattanfifth, manta, Marco.Simonc****, maxosini, michele2508, michele_giann****, mir59to, m.guerreschi, Mr.Crocodile, nciusca, nusan, odo, OiPaz, outcry, paoloR, pietroki, Pippo S., Poppy, psycheye, rodri, rscasse, rudy69, rutger82, ryogazero, sergiob***a, sverx, teodoro.sallu***, TheProf, toto200, van_fanel, Zane (*www.zanezane.net*), Zet, Zibis.
- **Nomi:** Maurizio Antonelli (*www.maury.it*), Paolo Avallone, Renata Bagnasco, Stefano Bellezza, Mario Benedetto, Paul Berthelot, Carla Bertinelli, Gian Marco Bezzi, Luca Bianucci, Roberto Bolzan, Dario Bonacina, Giovanni Briolini, Renato Caluzzi, Antonio Paolo Carbone, Francesco Caravenna, Fabio Chiodo, Paolo Copello, Cristina Corti, Roberto Danzo, Lucio "LuX" De Carli, Riccardo De Servi, Lia Desotgiu, Andrea Domenici, Lello Esposito, Giovanni "Jax" Formentini, Giulio Fornasar, Daniele Forsi, Alessandro Giardina, Gabriella Gregori, Davide La Valle, Pierluigi Lenoci, Stefano Luciani, Stefano Malagigi, Stefano Menozzi, Luca Martino, Andrea Montesi, Giacomo Mussini, Mauro Ongaro, Andrea Pernarella, Nilo Radicchi, Daniele Raffo, Giuseppe Regalzi, Simone Ruggeri, Daniele Russolillo, Luigi Sandon, Matteo Schiavini, Corrado Sferragatta, Filippo "Hytok" Simone, Vittorio Sozzi, Piergiorgio Traversin, Moreno Trinca, Walter Tross, Carlo Vaccari, Dario Villone, Federico Zoppelli (Doc), Federico Zuccardi Merli.

Aggiornamenti nella Rete

La sicurezza informatica è in continua evoluzione: per questo il testo de *L'Acchiappavirus* è disponibile integralmente su Internet, insieme agli ampliamenti e aggiornamenti che man mano si renderanno necessari, presso il mio sito *www.attivissimo.net*.

Siete pronti? Siete caldi?

Guardatevi. State leggendo un libro di sicurezza informatica: l'avreste mai detto? Compiacetevi e poi voltate pagina.

Questo libro è stato scritto su computer Linux, Mac e Windows usando il programma libero e gratuito OpenOffice.org*. Nessun programma Microsoft è stato maltrattato durante la sua realizzazione.*

Capitolo 2
Là fuori è una giungla

I giornalisti di stampa e TV si buttano a pesce sulle periodiche invasioni di virus. Spesso lo fanno con superficialità e incompetenza, per cui è facile che a furia di ascoltarli abbiate una percezione distorta della sicurezza informatica.

Se questo è il primo libro d'informatica che prendete in mano, preparatevi a buttar via molti dei luoghi comuni che vi hanno propinato sin qui. Eccone alcuni:

- **La sicurezza è un problema occasionale**, per cui non vale la pena di darsi troppo da fare. Falso. Dietro a ognuno dei virus che fanno notizia nei *media* di larga diffusione, perché fanno sconquassi su vasta scala, c'è una miriade di altri virus altrettanto micidiali che però non si propagano a sufficienza da meritarsi un titolo di giornale. Quanti virus nuovi escono ogni anno, secondo voi? Cinque o sei? Dieci? Siete fuori strada: in certi periodi ne esce **uno nuovo ogni giorno.**
  Per esempio, a marzo 2004 il produttore di antivirus Sophos ha aggiornato il proprio prodotto per riconoscere 824 nuovi virus, portando il totale riconosciuto a 89.112. Circa il 90% di questi virus ha una circolazione quasi nulla al di fuori degli ambienti specialistici, per cui è praticamente irrilevante, ma anche così resta uno zoccolo duro di un migliaio di virus ad alta diffusione. Sempre Sophos, a maggio 2004, ha analizzato ben 959 nuovi virus, il numero più alto in un mese da dicembre 2001[4].
- **L'unico pericolo è costituito dai virus: basta un buon antivirus e il gioco è fatto**. Purtroppo non è così. Quando collegate il vostro computer a Internet, tutta Internet si collega a voi, e là fuori ci sono vandali che non hanno di meglio da fare che cercare a casaccio computer vulnerabili da devastare. Molti lavorano per i pubblicitari senza scrupoli di Internet, i cosiddetti *spammer*: cercano di penetrare nel vostro computer per trasformarlo in un disseminatore occulto di e-mail pubblicitari.[5] Questi aggressori non hanno bisogno di virus per agire. Possono approfittare di un difetto in uno dei programmi che usate, oppure imbrogliarvi creando siti-trappola, e-mail ingannevoli o

programmi che vi spiano. **Ci sono mille modi per insinuarsi in un computer; i virus sono soltanto un grimaldello fra tanti**.

- **Nessuno ce l'ha con me, per cui non ho nulla da temere.** Come già accennato, nella maggior parte dei casi è vero che nessuno ce l'ha con voi: gli attacchi personali mirati sono rari. Ma questo non vuol dire che siete al sicuro. Infatti virus e aggressori sparano nel mucchio: sono come ladri che provano la maniglia di tutte le porte del quartiere per vedere se per caso qualcuna è stata lasciata aperta. A loro non interessa chi siete. Di conseguenza, **chiunque è a rischio di attacco**.
- **Ma cosa vuoi che mi succeda? È solo un computer**. Certo: un computer che però contiene sicuramente molti dati personali o riservati. Per esempio, un intruso può rubarvi i codici di accesso al vostro abbonamento Internet e spacciarsi per voi, magari mandando un e-mail di insulti al vostro capo; se usate il computer per gestire i vostri conti correnti, potrebbe prosciugarveli. Potrebbe infettarvi il computer con programmi che compongono numeri a pagamento, tipo gli 899, causandovi un salasso in bolletta. Potrebbe depositarvi immagini pornografiche o pedofile e poi ricattarvi con la minaccia di segnalarle a familiari e magari alla magistratura: è una nuova forma di crimine in forte aumento. E queste sono solo le prime cose che mi vengono in mente.
- **Ho l'ultima versione di Windows, sono invincibile.** È logico pensare che il prodotto dell'azienda di maggior successo della storia dell'informatica debba essere il meglio che offre il mercato, affinato da decenni di ricerca e sviluppo. Purtroppo non è così. È sufficiente un e-mail o un sito Web appositamente confezionato per devastare Windows, se non lo irrobustite. **Qualsiasi versione di Windows XP distribuita prima di settembre 2004 è infettabile semplicemente visualizzando un'immagine**[6] [7]. Posso organizzarvi una dimostrazione pratica di falle come queste, se non ci credete.

Piccoli sporchi segreti

Uno dei segreti più importanti di tutta Internet è che **il mittente di un normale e-mail non è garantito**.

Falsificare il mittente di un normale e-mail è facilissimo e non richiede alcun programma apposito o conoscenze arcane: basta immettere dati falsi nell'impostazione del vostro programma di posta e anche voi potrete disseminare e-mail apparentemente provenienti dagli indirizzi più disparati, come mostrato in Figura 2.1.

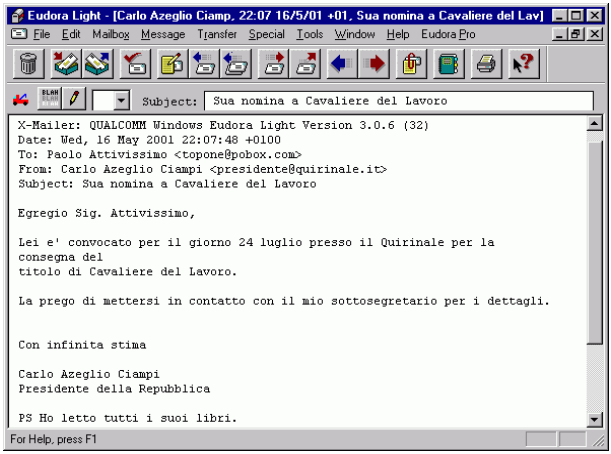

Figura 2.1

Questa magagna (dovuta al fatto che Internet in origine era uno strumento riservato ai ricercatori e quindi non esisteva il problema degli abusi e dell'autenticazione) è la chiave di infinite truffe, di quasi tutti gli attacchi di virus e di molte intrusioni informatiche.

- Ogni giorno, milioni di utenti ricevono e-mail che sembrano provenire da Microsoft e consigliano di aprire subito il file allegato al messaggio *"per ragioni di sicurezza"*: l'allegato è in realtà un virus, ma l'autorevolezza della fonte apparente fa mettere da parte ogni dubbio.
- Ogni giorno, milioni di clienti di banche e servizi di acquisto via Internet ricevono e-mail apparentemente inviati dal servizio clienti, contenenti inviti a visitare il sito della banca o del servizio per *"aggiornare i propri dati"*: in realtà sono messaggi inviati in massa da truffatori che creano un falso sito, nel quale le vittime immettono i propri codici segreti, pensando di essere nel sito autentico. È l'equivalente Internet della famosa truffa con il falso Bancomat.

  Gran parte di questi tentativi fallisce, ma alcuni vanno a segno:

nel 2003 il solo governo USA ha raccolto cinquecentomila denunce di furto d'identità, per un totale sottratto di quattrocento milioni di dollari.[8] [9]

- Ogni giorno, migliaia di dipendenti di aziende ricevono un e-mail dal loro capo (o almeno così sembra) che li invita a installare un "nuovo programma". Il capo ordina, dunque il dipendente esegue: ma il capo non c'entra niente, e il "nuovo programma" è in realtà un grimaldello che consente a chi si è spacciato per il capo di entrare e uscire a proprio piacimento dal computer della vittima e da lì raggiungere gli altri computer dell'azienda per spionaggio o devastazione.

Ricordate: **il mittente di un normale e-mail non è garantito**. Non dimenticatelo mai. Esistono tecnologie che consentirebbero di autenticare il mittente, ma per ora non vengono usate nella corrispondenza elettronica standard. Ci sono vari metodi tecnici per capire se un mittente è falso, ma le vostre armi migliori restano prudenza e buon senso.

Il computer colabrodo

Un altro segreto importante è che **Windows, se non lo addomesticate, è un vero colabrodo e rema contro di voi.** La pubblicità di certo non lo dice, ma lo dimostrano i frequentissimi bollettini di sicurezza[10] pubblicati da Microsoft stessa e la documentazione dell'indagine antitrust dell'Unione Europea.[11] Quasi tutti i bollettini si concludono con la fatidica frase *"può consentire l'esecuzione di codice arbitrario"*, che è un eufemismo per dire che la falla consente a qualunque vandalo di far fare al vostro computer quello che gli pare.

Grazie a virus come *Blaster* e *Sasser,* **per infettare un computer Windows è sufficiente collegarlo a Internet.** Non occorre visitare siti o scaricare messaggi di posta. Per questa e altre ragioni, **un computer Windows non va mai collegato a Internet prima di adottare una serie di precauzioni**, descritte nelle pagine successive di questa guida.

Certo anche le alternative a Windows non sono perfette, ma il prodotto Microsoft è di gran lunga più carente e vulnerabile. Scettici? Chiedete ai vostri amici che usano computer Apple o Linux quanti virus hanno preso di recente.

Non è che in Microsoft siano cretini: semplicemente, gli atti del processo antitrust statunitense e dell'istruttoria dell'Unione Europea che hanno visto coinvolta la società di Bill Gates hanno dimostrato che presso Microsoft (e anche altrove) le ragioni commerciali hanno prevalso per anni sulla buona progettazione.

Ora, lentamente, si sta invertendo questa sciagurata tendenza, ma il lavoro di ristrutturazione è ancora lontano dall'essere completato. Nel frattempo, Windows rimane vulnerabile. **Prendere coscienza di questa vulnerabilità di Windows è il primo passo per porvi rimedio.**

Riconoscere i sintomi di un attacco

Ecco alcuni dei sintomi più frequenti di un'infezione o di un tentativo di intrusione. Vista la ben nota instabilità di Windows, la presenza di questi sintomi **non garantisce** che si tratti di un'infezione, ma significa comunque che è il caso di fare qualche verifica.

- **Riavvio spontaneo.** Windows ha una nota tendenza a piantarsi con la celebre schermata blu (è successo anche a Bill Gates durante una conferenza, nel 1998)[12], ma se succede troppo spesso (più di una volta al giorno) e Windows non si blocca ma si riavvia, è possibile che ci sia di mezzo un virus.
- **Antivirus disattivato.** Molti virus sono abbastanza astuti da disattivare gli antivirus. Se lo trovate disattivato senza motivo, cominciate a insospettirvi.
- **Programmi che non funzionano.** Anche un programma che si avvia e poi si blocca, mentre prima funzionava benissimo, è uno dei più frequenti indicatori di infezione.
- **Computer lentissimo.** Un avvio di Windows che richieda più di tre-quattro minuti è un brutto segno, ma potrebbe anche essere dovuto a un elevato numero di programmi che si avviano da soli all'avvio: vale la pena di verificare. Se il computer ci mette più di cinque minuti per partire ed è visibilmente più lento di quando l'avete comprato, il segno è bruttissimo.
- **Internet lenta.** Se la vostra connessione alla Rete vi sembra molto più lenta del solito, è possibile che un virus la stia usando di nascosto per disseminare copie di se stesso, ma è anche possibile che abbiate semplicemente avviato un

programma di scambio file (come Kazaa, WinMX, BitTorrent e altri) il cui traffico intasa la connessione.

- **Spazio su disco esaurito.** Alcuni vandali penetrano nei computer per usarli come deposito insospettabile della loro refurtiva digitale (immagini, programmi, film, musica). Così, se vengono arrestati e il loro computer viene perquisito, non hanno addosso nulla di compromettente; siete voi che ce l'avete in casa o in ufficio. I file sono di solito depositati in modo invisibile alla vittima, ma ovviamente occupano spazio lo stesso, per cui vi ritrovate con il disco pieno e non sapete perché.
- **Il vostro computer vuole giocare alla guerra termonucleare globale.** Calma, calma, sto scherzando! Non avete visto *Wargames*?

Lo stacca-e-attacca contro gli attacchi

Non disperatevi: quasi tutte le più gravi magagne di Windows si possono curare (o perlomeno incerottare). I rimedi si riassumono in poche regole, che ho pomposamente intitolato *Dodecalogo di sicurezza*. Trovate il Dodecalogo in una pagina a parte, in modo che possiate staccarlo oppure, se trovate sacrilego mutilare un libro, fotocopiarlo e appenderlo accanto al PC come promemoria.

Probabilmente molte delle regole del Dodecalogo vi sembreranno inizialmente impraticabili, esagerate, insensate e stupide. Non pretendo che mi crediate sulla parola. I prossimi capitoli servono proprio per spiegare le ragioni di queste norme e il significato di alcuni termini che per ora possono risultare poco chiari.

Per ora, tenete presente semplicemente che **da sole, queste dodici regole vi avrebbero tenuto al riparo da tutti gli attacchi informatici degli ultimi anni,** consentendovi di navigare tranquilli e senza limitazioni. Non so voi, ma io direi che è un bel risultato.

Piccolo dodecalogo di sicurezza

(da staccare e appendere accanto al computer)

1. Installate un buon **firewall**.
2. Installate un buon **antivirus**, tenetelo costantemente **aggiornato** e usatelo su **tutti** i file che ricevete.
3. Fate il **backup** (almeno) dei vostri dati. Fatelo **spesso**. Fatelo **SEMPRE**.
4. Installate gli **aggiornamenti** (*patch*) di Microsoft.
5. Non installate software **superfluo** o di dubbia provenienza.
6. **Non usate Internet Explorer e Outlook Express.** Sostituiteli con prodotti alternativi più sicuri.
7. **Tenete disattivati ActiveX, Javascript e Visual Basic Scripting.** Riattivateli soltanto quando visitate siti di indubbia reputazione.
8. **Non aprite gli allegati non attesi, di qualunque tipo, chiunque ne sia il mittente**, e comunque **non apriteli subito**, anche se l'antivirus li dichiara "puliti".
9. **Non fidatevi dei link a banche o negozi forniti da sconosciuti.** Possono essere falsi e portarvi a un sito-truffa. Usate invece i Preferiti o il copia-e-incolla, oppure digitateli a mano, in un browser sicuro.
10. **Rifiutate la posta in formato HTML e non mandatela agli altri**. Usate il testo semplice, molto più sicuro.
11. **Non distribuite documenti Word:** trasportano virus e contengono vostri dati personali nascosti.
12. **Non fidatevi dei messaggi di allarme diffusi da stampa generalista, amici e colleghi**, e non diffondeteli, se non sono documentati.

Capitolo 3
Raddrizziamo Windows

Vi sarete forse accorti che nonostante le promesse dei venditori, Windows non è quel che si dice "facile da usare": ha più tic ed eccentricità di un *gentleman* britannico, ed è assai più stizzoso.

Quello che forse non sapete è che **Windows lavora contro di voi**. Non siete voi a essere scemi: **è lui che è un po' tardo**. Ditemi voi, per esempio, perché per *spegnere* Windows si pigia il pulsante START. Visto? È un complotto.

> ***Non sentitevi mai inferiori alla macchina.*** *Se una macchina, quando la si usa secondo le istruzioni e il buon senso, non fa quello per cui è stata progettata, non è colpa dell'utente; è colpa di chi l'ha concepita usando le parti meno nobili del proprio corpo o pensando al proprio portafogli invece che all'utente.*

Il fatto ineludibile, che tutti cercano di nascondere dando la colpa all'utente, è che **Windows è progettato male**. Non è una mia opinione personale; è un giudizio condiviso dalla stragrande maggioranza degli esperti del settore.

I progettisti di Windows (o meglio i responsabili del suo marketing) hanno ripetutamente fatto delle scelte precise che lo rendono letteralmente insidioso da usare anche per un utente esperto. Un comportamento apparentemente del tutto innocuo può causare disastri. Usare Windows così come viene venduto, senza dargli un'abbondante raddrizzata, è come guidare un'auto in cui se aprite il posacenere mentre ascoltate la radio, ogni tanto si staccano tutte e quattro le ruote.

Purtroppo, per una lunga serie di ragioni, con Windows bisogna convivere (anche se con un po' d'impegno si può quasi sempre migrare ad alternative come Mac o Linux, come ho fatto io). Si può comunque fare molto per renderlo un po' meno stizzoso e vulnerabile.

> *Le istruzioni date qui si riferiscono a Windows XP Home italiano installato nella maniera più diffusa, ossia con un unico utente che ha privilegi di amministratore. Per le in-*

stallazioni multiutente e/o con utente senza questi privilegi, in genere è sufficiente ripetere gli stessi passi per ciascun utente oppure eseguirli dopo aver acquisito i privilegi di amministratore.

Se non avete capito nulla del paragrafo precedente, probabilmente il vostro computer è configurato nella maniera più diffusa e quindi non dovete preoccuparvi di questo mio momentaneo delirio terminologico.

Aiuto, mi sono perso

Per riprendere il controllo del computer bisogna sapersi orientare nei suoi meandri, ma è difficile farlo quando le informazioni che ci servono ci vengono **volutamente nascoste**. Ebbene sì, Windows fa questo e altro.

Vi chiedo quindi di dedicare qualche minuto a una personalizzazione di Windows che lo renderà un po' meno restio a dirci cosa sta succedendo davvero dentro il computer e definisce un punto di partenza standard dal quale costruire la necessaria blindatura. Non posso spiegarvi la strada per la salvezza se partite da posti diversi: troviamoci tutti in uno stesso luogo, con la stessa attrezzatura, e partiamo da lì, OK?

Le prossime pagine contengono consigli che non producono direttamente sicurezza, ma servono a creare un ambiente adatto per ottenerla. È un po' come quando andate a scuola guida: la prima cosa che vi consigliano è accomodare il sedile e regolare gli specchietti.

Menu di plastica

Cominciamo proprio dal **pulsante Start.** Windows XP, nel tentativo di "semplificarvi" la vita, ha un nuovo menu Start tutto plasticoso e ridotto all'osso: contiene soltanto i programmi che Microsoft vuole indurvi a usare (guarda caso, tutti prodotti Microsoft). Le cose che mamma Microsoft ha deciso che non vi devono interessare troppo sono relegate dietro la scritta *"Tutti i programmi"* (Figura 3.1).

Quest'impostazione nuova è una vera pena per chi proviene da edizioni precedenti di Windows, ma disorienta anche chi si avvicina a Windows per la prima volta, perché richiede tantissime cliccate per fare qualsiasi cosa diversa da ciò che Windows ha deciso che volete fare.

Figura 3.1

Come se non bastasse, Windows riordina da solo i menu in base alla frequenza con cui usate i programmi, per cui non trovate mai le cose allo stesso posto. È come convivere con un *poltergeist*.

Niente panico: rimettiamo subito le cose com'erano ai vecchi tempi e togliamo la crosta luccicante per rivelare il *vero* menu Start.

Cliccate con il pulsante **destro** del mouse su *Start* e scegliete *Proprietà*. Nella scheda *Menu di avvio*, cliccate su *Menu di avvio classico* in modo che vi compaia un pallino e poi cliccate su *OK*. Fatto questo, cliccando su *Start* otterrete il menu Start completo "classico" mostrato in Figura 3.2. State cominciando a far capire a Windows chi comanda.

Per riportare al suo aspetto "tradizionale" anche il Pannello di Controllo, aprite la relativa finestra nel menu Start (Start > Impostazioni > Pannello di controllo) e cliccate su *Passa alla visualizzazione classica*.

Se volete riportare Windows XP a un look ancora più simile a quello dei vecchi Windows che vi sono familiari,

scegliete Start > Impostazioni > Pannello di controllo > Schermo > Temi e selezionate Windows classico*. Gli effetti plasticosi spariscono d'incanto.*

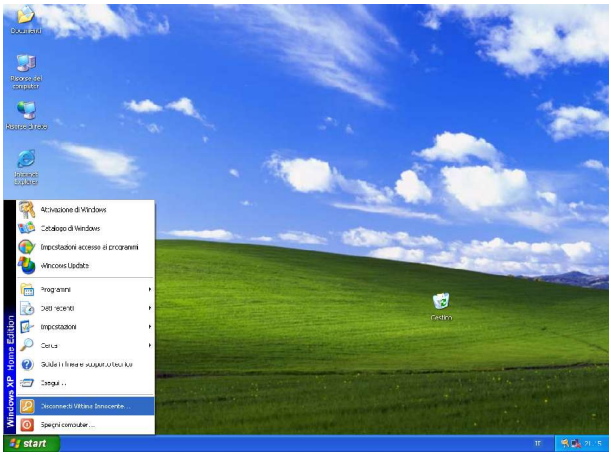

Figura 3.2

Levare il paraocchi al maggiordomo

Lo strumento essenziale per orientarsi e poi piegare Windows al vostro volere è il programma *Esplora risorse* (da non confondere con *Risorse del computer*), che vi permette di visualizzare l'organizzazione dei dati e dei programmi nel computer, cambiare i nomi ai file, cancellarli e spostarli con facilità. È il vostro maggiordomo, anche se un po' carente in fatto di trasparenza e *aplomb*.

Esplora Risorse è nascosto: bisogna tirarlo fuori, scegliendo *Start > Programmi > Accessori > Esplora Risorse*. Averlo così fuori mano è scomodissimo, dato che lo userete molto spesso, per cui conviene metterlo dove fa comodo a voi e non a Windows, ossia nella sezione principale del menu Start.

Per farlo, scegliete *Start > Programmi > Accessori > Esplora Risorse* ma *non cliccate* sul nome del programma: lasciate aperta la serie di menu. Cliccate con il pulsante sinistro del mouse su

Esplora risorse, tenete premuto il pulsante e spostate il mouse verso la zona superiore della sezione principale del menu Start.

Notate che un "fantasma" della voce *Esplora risorse* segue il mouse: in gergo tecnico, state *trascinando* un elemento di Windows. È una cosa che farete tantissimo e che probabilmente sapete già fare, ma vale la pena di segnalarne adesso il nome ufficiale, così non dovrò farlo in seguito.

Quando arrivate sopra la sezione principale del menu Start, nel menu compare una linea orizzontale nera: indica dove verrà inserita la voce *Esplora risorse*. Quando la linea è in una posizione di vostro gradimento, rilasciate il pulsante del mouse: nel menu Start compare Esplora Risorse, pronto all'uso e accessibile con la metà delle cliccate normalmente necessarie.

La tecnica che avete appena usato viene usata anche in moltissime altre occasioni per riordinare i programmi secondo i vostri gusti personali, in modo da avere a portata di mano tutto quello che serve invece di dovervi perdere in caterve di cliccate a vanvera.

> *Se siete il tipo di persona che si ricorda le combinazioni di tasti, potete stupire i vostri amici patiti del mouse usando una scorciatoia ancora più rapida per lanciare Esplora Risorse: premete il tasto con il simbolo di Windows (nella zona inferiore sinistra della tastiera) e contemporaneamente la lettera E.*

Ora che abbiamo il nostro "maggiordomo" a portata di mouse, è giunta l'ora di metterlo al lavoro. Lanciate Esplora Risorse (*Start* > *Esplora risorse* oppure premete la combinazione di tasti Windows+E).

La schermata di Esplora Risorse (Figura 3.3) è divisa in due parti, che rispecchiano l'organizzazione dei dati e dei programmi nel computer.

- A sinistra, acquattato dentro *Risorse del computer*, c'è l'elenco dei dischi rigidi e dei lettori di CD e DVD del computer. Cliccando su ciascuno di questi dispositivi, a destra ne viene visualizzato il contenuto, organizzato in *cartelle* (che i vecchi bacucchi dell'informatica come me chiamano *directory*). Queste cartelle contengono i file (documenti o programmi) o altre "sottocartelle". La zona di sinistra di Esplora Risorse mostra tutte queste

suddivisioni in una mappa logica che ha la forma di una radice d'albero.

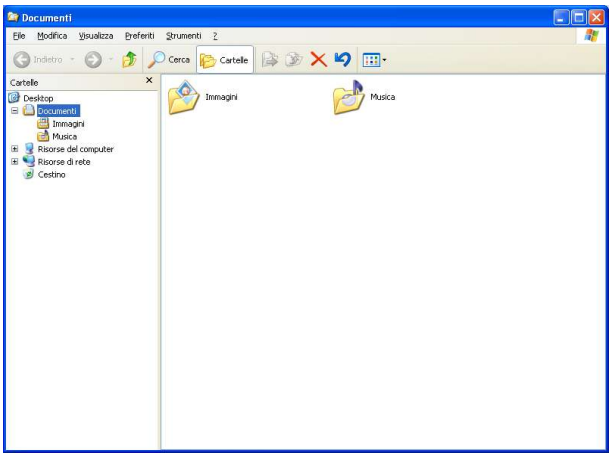

Figura 3.3

- La zona di destra, invece, mostra il contenuto della cartella che è selezionata in quel momento (perché vi avete cliccato sopra); la potete riconoscere perché è l'unica che ha l'aspetto di una cartelletta aperta.
  Se cliccate sull'icona del disco rigido C:, può darsi che intervenga come al solito mamma Microsoft, dicendovi che ci sono cose che non dovete guardare e sapere. *"Questi file sono nascosti... Non modificare il contenuto della cartella"*.
  Il consiglio è valido, anche se un po' iperprotettivo: non viene permesso neppure di *guardare* senza toccare, che è quello che vi servirà fare tra poco. Cliccate dunque su *Visualizza contenuto della cartella* ogni volta che vi imbattete in questo altolà; se qualcuno protesta, dite che vi mando io.

  > *A proposito di "guardare senza toccare": circola da anni un allarme secondo il quale un file di nome* jdbgmgr.exe *o* sulfnbk.exe*, contenuto nella cartella di Windows, sarebbe un pericolosissimo virus da cancellare. Non abboccate! È una bufala.*
  >
  > *Ricordate inoltre che i programmi non si disinstallano cancellando le loro cartelle: bisogna andare nel Pannel-*

lo di Controllo e usare l'apposita funzione di rimozione programmi.

Windows non ha ancora finito di trattarci da bambini pasticcioni e continua a nasconderci molti elementi essenziali del suo funzionamento. Lo so, l'aspetto spoglio iniziale di Windows dà un'impressione di semplicità e ordine, ma vi garantisco che è soltanto un'impressione. Come dice il proverbio, una scrivania spoglia è sintomo di un cassetto stracolmo alla rinfusa.

Selezionate una cartella qualsiasi, per esempio *Windows*: nella zona di destra compare un elenco di cartelle e di file dai nomi più o meno indecifrabili. Adesso è giunto il momento di scostare le tende e vedere cosa c'è *davvero* nel vostro computer. Non è un bello spettacolo, ma è necessario affrontarlo (Figura 3.4).

In Esplora Risorse, scegliete il menu *Strumenti* e la voce *Opzioni cartella*. Nella finestra che compare, scegliete la scheda *Visualizzazione*.

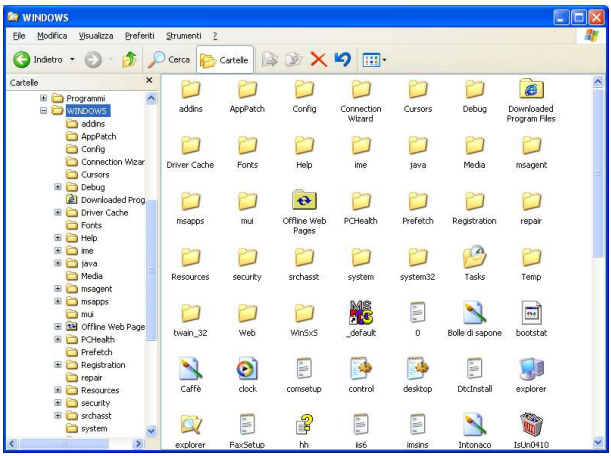

Figura 3.4

Impostate le voci seguenti, lasciando invariate le altre (Figura 3.5):

- ☑ *Visualizza cartelle e file nascosti*
- ☐ *Memorizza le impostazioni di visualizzazione di ogni cartella*

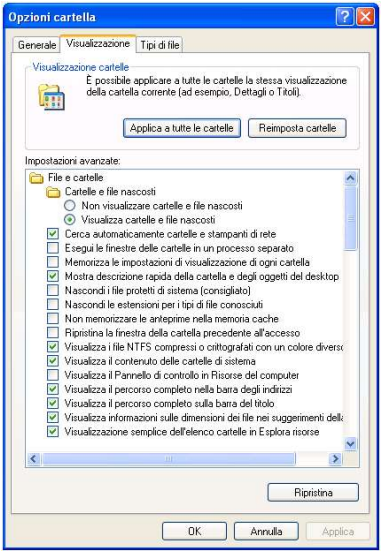

Figura 3.5

- ☐ *Nascondi i file protetti di sistema* (Windows protesta, ma rispondete cliccando su *Sì*)
- ☐ *Nascondi le estensioni per i tipi di file conosciuti*
- ☑ *Visualizza il contenuto delle cartelle di sistema*
- ☑ *Visualizza il percorso completo sulla barra del titolo*

Cliccate sul pulsante *Applica a tutte le cartelle* e rispondete *Sì* alla richiesta di conferma. Infine cliccate su *OK*.

Se ora esplorate una cartella qualsiasi, noterete che sono "comparsi" file e cartelle in gran numero. In realtà c'erano già, soltanto che Windows ve li nascondeva. **Non toccate niente:** per ora si tratta soltanto di sapere dove stanno le varie cose che in seguito vorrete modificare e addomesticare.

Sempre in Esplora Risorse, scegliete *Visualizza* > *Barra di stato*: questo fa comparire, lungo il bordo inferiore della finestra di Esplora Risorse, una barra che contiene informazioni utili, come lo spazio disponibile su disco e lo spazio occupato da ciascuna cartella o raggruppamento di file (Figura 3.6).

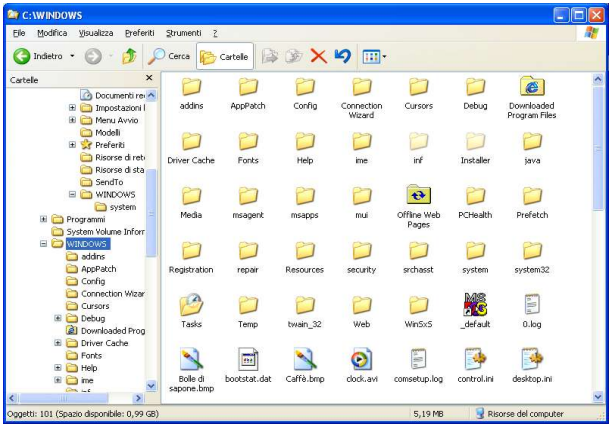

Figura 3.6

*Molti utenti, per aumentare la compattezza e completezza delle informazioni presentate da Esplora Risorse, scelgono la visualizzazione dei dettagli (*Visualizza > Dettagli*).*

Quest'impostazione ha il vantaggio di mostrare subito la data di modifica di ciascun file, mentre nella visualizzazione standard (chiamata Titoli*) la data di modifica viene visualizzata soltanto posizionando il mouse sopra il file che vi interessa.*

È questione di gusti: se preferite vedere i dettagli, ricordatevi di applicare questa preferenza a tutte le cartelle, scegliendo Strumenti > Opzioni cartella > Visualizzazione > Applica a tutte le cartelle*.*

C'è un'ottima ragione per la quale vi ho fatto fare questa trafila e adesso il vostro Windows gira con tutte le frattaglie in mostra: **i pericoli principali vengono proprio da queste cose nascoste**, perché gli aggressori sfruttano questa loro natura normalmente invisibile. Ora sono costretti a tentare di fregarvi alla luce del sole, senza l'aiuto delle cortine fumogene di mamma Microsoft.

Il file travestito

Una delle "cortine fumogene" più irritanti e pericolose di Windows è il suo vezzo di **nascondere le estensioni** dei nomi dei file. L'*estensione* è un pezzetto del nome di un file, separato dal resto da un punto: è una sorta di "cognome", nel senso che conoscendolo si sa a che famiglia appartiene, ossia di che tipo è, un determinato file.

> *Presso* www.filext.com *trovate un ricchissimo elenco di estensioni che spiega il tipo di file corrispondente a ciascuna estensione. L'elenco è in inglese, ma ne esistono equivalenti italiani, facilmente reperibili digitando in Google.it le parole* estensioni file*.*

Windows si basa quasi esclusivamente sulle estensioni per decidere come gestire un file. Per esempio, normalmente i documenti scritti da Microsoft Word hanno l'estensione "*.doc*", per cui un documento avrà un nome del tipo *Documento.doc.*

Quando Windows vede l'estensione *.doc*, ne deduce che si tratta di un documento Word e lo apre con Word; quando vede l'estensione *.txt*, presume che si tratti di un documento di testo semplice e lo apre con il Blocco Note; e così via.

È grazie a questo meccanismo che quando fate doppio clic su un file parte magicamente il programma apposito per quel tipo di file. Ma **Windows normalmente nasconde queste estensioni**, per cui sullo schermo il file *Documento.doc* appare semplicemente come *Documento*.

Chi se ne frega, direte voi. Invece questo comportamento di Windows è letale, perché ci impedisce di riconoscere correttamente i file e quindi distinguere quelli buoni da quelli cattivi.

Torniamo un attimo al paragone del cognome. Immaginate di sapere che Giovanni Cazzulati è un bravo ragazzo (martoriato peraltro da un cognome infelice) e che Giovanni Rezzonico è un delinquente. Suona il campanello: chi è? *"Giovanni*", risponde una voce. Senza sapere il cognome, come fate a sapere chi sta per entrarvi in casa?

Questo è esattamente quello che fa normalmente Windows: **nascondendo il "cognome" dei file, ossia la loro estensione, vi sottrae uno dei metodi più semplici e diretti di distinguere fra**

bravi e cattivi. Sapete perché lo fa? Semplicemente perché qualche mago del design ha deciso che quei *"puntoqualchecosa"* in fondo ai nomi sono antiestetici. Facciamoli sparire, e al diavolo le conseguenze.

Ma le conseguenze sono serie. Windows non controlla il *contenuto* di un file: si fida quasi esclusivamente della sua estensione. Se gli date in pasto un file qualsiasi, purché abbia l'estensione *.doc*, lui lo apre automaticamente con Word, *anche se non è un documento Word*.

Fate una prova pratica:

- prendete un file scritto con Word o Wordpad e cambiategli l'estensione da *doc* a *txt*.
- Ottenete un messaggio di avvertimento: confermate l'intenzione di cambiare estensione.
- Se fate doppio clic su questo file, ora viene aperto dal Blocco Note (con risultati incomprensibili), non da Word/Wordpad: eppure il contenuto del file non è affatto cambiato.

Peggio ancora, se Windows vede un file che ha l'estensione *exe o com*, per esempio, presume che si tratti di un file eseguibile (un programma) e **gli affida ciecamente il controllo completo del computer**, con rischi facilmente intuibili.

> *Sentirete spesso parlare di "file eseguibili". È un termine da tenere ben presente, perché i file eseguibili sono quelli più pericolosi. I virus, per esempio, sono file eseguibili; lo sono anche i programmi normali, come Word o Outlook.*
>
> *Ma cosa vuol dire esattamente* eseguibile*? Semplice: un file eseguibile è un file che, quando lo attivate, fa qualcosa* autonomamente: *esegue le istruzioni del suo creatore, che possono essere ostili.*
>
> *I file non eseguibili, invece, sono inerti e si limitano a contenere dei dati: quando li attivate (per esempio con un doppio clic), non fanno nulla se non chiamare un programma che li legga e per questo sono considerati poco pericolosi.*

Musica, immagini e documenti, per esempio, sono file non eseguibili. Tuttavia possono essere manipolati in modo da contenere istruzioni ostili, quindi vanno comunque trattati con cautela.

Grazie a questa furbata di nascondere le estensioni, se un aggressore vi manda un virus e lo chiama *donninenude.exe,* Windows ve lo presenterà semplicemente come *donninenude*. Come fate a sapere se è un programma (quasi sicuramente pericoloso) o un'immagine (probabilmente ma non necessariamente sicura)? Non potete fidarvi neppure dell'icona accanto al nome, perché è facilmente falsificabile. Usare un nome allettante, fra l'altro, è uno dei classici espedienti psicologici degli aggressori.

Se le estensioni sono nascoste, non avete modo di sapere, insomma, che cosa farà Windows se fate doppio clic su un file. Il file potrebbe essere aperto dal visualizzatore di immagini di Windows o da un altro programma, ma potrebbe anche essere *eseguito*, ricevendo quindi il pieno controllo del vostro computer, con facoltà di fare quello che vuole: cancellare o alterare file, rubarvi dati personali, infettare altri computer, mandare e-mail falsi a vostro nome, addebitarvi telefonate a numeri porno e chi più ne ha più ne metta.

Se invece attivate la visualizzazione delle estensioni, come mostrato nelle pagine precedenti, e un aggressore vi manda un file "travestito" (per esempio un virus la cui icona è quella di un documento di Word ma la cui estensione è di quelle eseguibili), vi accorgerete dall'estensione che non si tratta di ciò che dice di essere ed eviterete il pericolo.

Quali sono le estensioni pericolose?

In realtà non si può parlare in termini assoluti di estensioni "pericolose" e "innocue". Con l'evolversi (per così dire) di Windows e dell'astuzia degli aggressori, tipi di file che un tempo erano assolutamente innocui sono diventati potenzialmente letali. Fino a qualche anno fa non era pericoloso ricevere un e-mail in formato HTML; ora lo è. Un tempo, l'idea di infettarsi aprendo un documento Word, un brano MP3, un'immagine o un videoclip avrebbe fatto sorridere. Ora no. Meraviglie del progresso.[13]

Di conseguenza, **nessuna estensione può essere considerata automaticamente sicura.** Ci sono però gradi diversi di probabile pericolosità: alcune estensioni vanno trattate con maggiore cautela di altre, perché sono quasi sicuramente ostili.

Le principali estensioni ad alto rischio sono queste:

- *bat, chm, cmd, com, cpl, dll, exe, hlp, hta, inf, lnk, ocx, pif, reg, scr, url, vbs* (ce ne sono molte altre, ma sono assai più rare)[14].

Se ricevete un allegato con una di queste estensioni, è quasi sicuramente un tentativo di aggressione. Cestinatelo immediatamente.

Più in generale, **se un file ha un'estensione che non corrisponde alla sua natura dichiarata, è da considerare automaticamente pericoloso** e va **cestinato senza esitazione**, **chiunque** (e sottolineo il *chiunque*) ne sia la fonte apparente.

Per esempio, se qualcuno vi manda un file dicendovi che si tratta di un'immagine ma l'estensione del file non è una di quelle usate dalle immagini (*jpg, gif, bmp, tga* e simili), è meglio alzare la guardia.

> *Se temete di non ricordarvi tutte queste estensioni nel momento del bisogno, potete usare un altro criterio più semplice: decidere che **qualsiasi file con un'estensione che non vi è familiare è pericoloso fino a prova contraria** e non va aperto con disinvoltura.*
>
> *Se vi imbattete in un file di cui non riconoscete l'estensione, quindi, evitate assolutamente di aprirlo facendovi sopra doppio clic e sottoponetelo all'esame di un antivirus aggiornato.*
>
> *Insomma, i file vanno trattati un po' come i funghi: se non li conoscete, non mangiateli sperando in bene, ma fateli controllare dall'ASL!*

Una volta attivata la visualizzazione delle estensioni, prenderete rapidamente dimestichezza con le estensioni dei tipi di file che usate più frequentemente (*jpg* per le immagini, *doc* per i testi, *pdf* per i documenti da distribuire, *mp3* o *wav* per la musica, eccetera). Se incontrate un file con un'estensione che non conoscete, per saperne di più potete consultare siti Internet come il già citato *www.filext.com*, dedicato alla catalogazione di tutte le estensioni conosciute.

Trucchi ostili con le estensioni

I creatori di virus e gli intrusi informatici sfruttano spessissimo trucchetti basati sulle estensioni. Molti virus assegnano ai file infettanti una ***doppia* estensione** (per esempio *megangale.jpg.exe*).

In questo modo, un utente poco attento che usa un Windows non "raddrizzato" non vede la seconda estensione (*exe*) che rivela il pericolo, ma soltanto la prima (*jpg*). Così, se ha familiarità con le estensioni, pensa che Windows le stia visualizzando correttamente, crede che il file sia un'immagine, lo apre con un doppio clic e si infetta.

> *Prendete l'abitudine di **cancellare subito e senza esitazioni qualsiasi file che trovate con una doppia estensione.** È quasi sicuramente un file ostile.*

Attivare la visualizzazione delle estensioni, insomma, aiuta a mettervi al riparo anche da questo classico espediente. Non è comunque una soluzione perfetta, come vedremo tra un attimo.

Un altro trucco molto diffuso fra gli aggressori è **separare le due estensioni mettendo molti spazi nel nome del file**, in modo da portare "fuori inquadratura" la vera estensione del file infettante. Per esempio, un virus può chiamarsi

"megangale.jpg .exe"

Nonostante le apparenze, questo è un **unico nome di file.** Gli spazi fra "*jpg"* e *".exe"* non devono trarre in inganno: fanno parte del nome. Se la finestra in cui visualizzate il nome del file è stretta, la seconda estensione sarà invisibile e verrete indotti a pensare che ci sia un'unica estensione, per di più una di quelle considerate poco pericolose (*jpg*), quando in realtà ce n'è un'altra quasi sicuramente ostile (*exe*).

*Ovviamente, **qualsiasi file che abbia queste caratteristiche è da considerarsi ostile e va cancellato subito.** La Figura 3.7 mostra un esempio di virus (Netsky) che ho ricevuto via e-mail, annidato dentro un file ZIP e travestito da documento (falsa estensione RTF).*

Figura 3.7

Un altro trucchetto in voga fra vandali e aggressori è approfittare dell'ambiguità fra *.com* come estensione di un file e *.com* come nome di sito. Per esempio, vi arriva un e-mail che contiene una frase del tipo *"Visita magacesira.com!!!"*. Sembra l'invito a visitare un sito e sembra che se cliccate sul nome del "sito" verrete portati al sito reclamizzato: in realtà la cliccata lancerà il programma *magacesira.com* allegato al messaggio, che infetterà il PC.[15]

Estensioni maledette

Purtroppo i difetti di progettazione di Windows non si esauriscono qui. Anche dopo aver chiesto *esplicitamente* a Windows di visualizzare le estensioni dei nomi dei file, il sistema *continua a nasconderne alcune*.

Questo, a casa mia, si chiama fare i dispetti. A dire il vero si chiama in un altro modo, ma questo è un libro per tutta la famiglia e mi devo trattenere.

Non ci credete? Provateci. Vi propongo una dimostrazione pratica da mostrare agli amici: creerete un "virus" (innocuo, non temete) che sfrutta questi difetti di Windows per travestirsi e ingannarvi nonostante tutto.

- In Esplora Risorse, andate nella cartella di Windows (di solito è *C:\WINDOWS*) e nella sottocartella *system32* e cercate un file di nome *calc.exe*, facilmente riconoscibile dall'icona che rappresenta una calcolatrice. È il programma *Calcolatrice* di Windows: un programmino assolutamente inoffensivo, che useremo come cavia non distruttiva.
- Copiatelo nella cartella *Documenti*: cliccate sul file usando il pulsante destro del mouse, scegliete *Copia*, cliccate sulla cartella *Documenti* in Esplora Risorse e scegliete il menu *Modifica* e la voce *Incolla*. Nella cartella *Documenti* avete ora una copia della Calcolatrice da sottoporre ai vostri esperimenti.
- Ora che avete attivato la visualizzazione delle estensioni e che sapete che il file *calc.exe* è un file eseguibile perché ha l'estensione *exe*, se lo riceveste o scaricaste da Internet, lo trattereste con cautela, giusto? Ma sareste meno cauti se avesse l'estensione *doc*, perché pensereste che si tratti di un documento di Word.

Adesso scatta l'infelice magia:

- Cliccate una sola volta sul file *calc.exe* e premete F2: questo vi consente di cambiare nome al file. Chiamatelo *calc.doc.pif*, ossia usate il trucchetto della doppia estensione usato da certi virus e descritto nelle pagine precedenti. Windows vi chiede di confermare il cambio di nome: fatelo.
- Zac, l'estensione *pif* non c'è più, anche se avevate detto a Windows di farvele vedere tutte. Sullo schermo avete il nome *calc.doc*: quello di un normale documento Word. Soltanto l'icona inconsueta vi può far venire qualche dubbio, ma il nome visualizzato no (e gli aggressori sanno come alterare anche l'icona). Se fate doppio clic su un file mascherato in questo modo, il file viene *eseguito* invece di essere aperto da Word. Visto che carognata?

Varianti dello stesso tranello si possono ripetere con altre estensioni, come *cnf, lnk, shb, url, scf e shs*. Queste estensioni non sono direttamente eseguibili (cliccandovi sopra, il file non viene eseguito), ma possono contenere per esempio l'istruzione di accedere automaticamente a un sito Web ostile che tenta di infettarvi o di comporre un numero telefonico a pagamento.[16] [17] [18]

Come vedete, ***non siete voi che siete imbranati con il computer: è Windows che vi tende le trappole****.*

A dire il vero, Windows ha in parte ragione. Alcune di queste estensioni dovrebbero in effetti restare nascoste, perché sono usate da Windows dietro le quinte (ad esempio, nelle voci del menu Start). Purtroppo bisogna fare delle scelte: finché stanno dietro le quinte, queste estensioni possono essere sfruttate da un virus; se le rendete visibili, sono decisamente bruttine. Prendere o lasciare.

Bloccati dal Blocco Note

C'è un trucchetto che vale la pena di usare per rendere meno pericolose certe estensioni comunemente usate dai virus: **associarle al Blocco Note**. In questo modo, se per caso fate doppio clic su un file che ha un'estensione nascosta, non verrà eseguito, ma semplicemente *aperto* (in modo innocuo) dal Blocco Note. Ecco come procedere:

1. Aprite *Esplora Risorse* e scegliete *Strumenti* > *Opzioni cartella* e da lì la scheda *Tipi di file*.
2. Sfogliate l'elenco dei tipi di file registrati e cercate l'estensione JS.
3. Cliccate su *Cambia* e scegliete il Blocco Note come programma da utilizzare per aprire tutti i file con quest'estensione. Cliccate su OK per confermare.
4. Ripetete i passi 2 e 3 per le seguenti estensioni: *jse, otf, reg, sct, shb, shs, vbe, vbs, wsc, wsf* e *wsh*.

Esiste anche un altro modo per convincere Windows a essere più onesto e non nascondervi nulla, ma comporta della chirurgia di precisione che potreste non sentirvi di fare: se vi interessa, è nella sezione del mio sito *www.attivissimo.net* dedicata a questo libro, in un capitolo supplementare intitolato *Per veri smanettoni*.

Non siete obbligati: è a questo che servono gli antivirus, che sono infatti in grado di riconoscere un virus anche se Windows gliene nasconde l'estensione. Se però volete togliervi la soddisfazione di addomesticare Windows, siete i benvenuti.

Estensioni stramaledette: CLSID

Anche dopo tutte queste modifiche, comunque, Windows ha delle falle che consentono a un aggressore di ingannarvi in fatto di estensioni. Esistono infatti i cosiddetti *CLSID*, che sono estensioni chilometriche racchiuse fra parentesi graffe, come questa:

{00020900-0000-0000-C000-000000000046}

Se prendete un file qualsiasi e gli assegnate questa estensione, Windows **non la visualizzerà**, nonostante tutte le modifiche descritte nelle pagine precedenti, ma penserà che si tratti di un documento Word (con tanto di icona di Word) e tenterà di gestirlo di conseguenza. Provare per credere (Figura 3.8).[19]

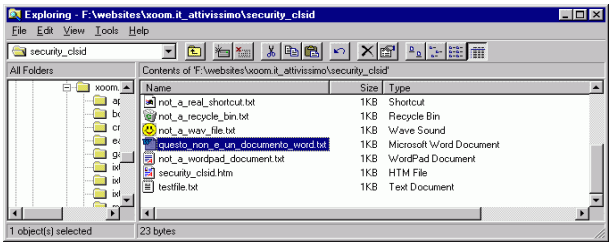

Figura 3.8

Chiaramente anche questo difetto può essere usato dai malintenzionati per confezionare file distruttivi che aggirano il semplice controllo basato sulle estensioni. È per questo che la Regola 8 del Dodecalogo sconsiglia di aprire (con il doppio clic) *qualsiasi* tipo di file ricevuto dall'esterno.

A mali estremi...

Insomma, **non c'è modo di convincere Windows a mostrarvi sempre la vera natura di tutti i file.** L'unico rimedio parziale a questa vulnerabilità è l'uso della finestra di MS-DOS, che però richiede che conosciate il buon vecchio sistema operativo DOS (un cui clone, chiamato *Prompt dei comandi,* è integrato in Windows sotto *Start* > *Programmi* > *Accessori*).

Se lanciate il *Prompt dei comandi* e lo usate per visualizzare il contenuto di una cartella contenente un file sospetto, verranno elencate tutte, ma proprio *tutte* le sue estensioni. Chiaramente è un modo assurdamente macchinoso per garantire l'identificazione

corretta di un file, ma può essere utile per i casi sospetti. Se non ve la sentite di fare tutte queste acrobazie, usate un antivirus: le farà lui per voi.

Prime tecniche di difesa: "Apri con"

Morale della favola: **in Windows "tal quale", non si può capire con assoluta certezza se un file è sicuro basandosi soltanto sulla sua estensione**. Però si può fare molto per indurlo a rendere più visibili i file pericolosi che si mimetizzano sfruttando le sue falle. Nei prossimi capitoli vedremo come risolvere definitivamente la parte residua del problema.

Nel frattempo, imparate a **non fare mai doppio clic su un file di provenienza meno che assolutamente affidabile**. Per esempio, non fate mai doppio clic su un file ricevuto via e-mail, chiunque sia (o sembri esserne) il mittente, neppure se si tratta di qualcuno che conoscete: è il metodo più classico per infettarsi con un virus.

Quando volete aprire un file, prendete l'abitudine di usare questa tecnica, che vi restituisce il controllo:

- Salvate sul disco rigido il file sospetto.
- Andate in Esplora Risorse e cliccate con il pulsante **destro** sul file.
- Compare un menu che contiene una voce *"Apri con"* (non *"Apri"* e basta, mi raccomando!). Cliccate su questa voce e scegliete il programma che corrisponde all'estensione apparente del file. State insomma scavalcando gli automatismi di Windows e decidendo manualmente quale programma usare per aprire il file sospetto.
- Se il programma che corrisponde all'estensione del file non riesce ad aprirlo o lo visualizza in modo incomprensibile, **cancellate il file: è quasi sicuramente infetto**, e se non è infetto è comunque danneggiato.[20]

Togliersi la pappa pronta di bocca

Windows fa di tutto per aiutarci: purtroppo, come Stanlio e Ollio, le sue intenzioni sono buone, ma l'esecuzione lascia un po' a desiderare. Per impedirgli di darci aiutini che in realtà spesso ci intralcia-

no, vi consiglio qualche altra modifica che non migliora necessariamente la sicurezza, ma rende Windows più agevole da usare.

Menu Start "ridotto"

In Windows XP, i sottomenu del menu Start sono "ridotti": compaiono soltanto le voci di utilizzo più frequenti (scelte da Windows). Le altre sono nascoste da una doppia freccia.

Questo significa che per andare a prendere i programmi usati meno frequentemente dobbiamo fare una gimcana di cliccate e che la disposizione delle voci nel menu Start cambia in continuazione, rendendo ancora più facile smarrirsi. Ancora una volta, Windows rema contro, insomma.

Per disattivare questa fastidiosissima funzione:

- fate clic con il pulsante destro del mouse sul pulsante Start, scegliete *Proprietà, Menu di avvio* e poi *Personalizza;*
- nell'elenco *Opzioni avanzate del menu di avvio*, togliete il segno di spunta (cliccandovi sopra) da *Usa menu personalizzati* (Figura 3.9);
- cliccate su *OK* e poi ancora su *OK*: i menu cessano di nascondere i programmi e di cambiarne continuamente la disposizione.

Figura 3.9

Area di notifica che si apre e chiude da sola

L'estremità destra della barra delle applicazioni, chiamata formalmente *area di notifica* o *System tray/Systray*, ospita spesso delle piccole icone, che servono a lanciare rapidamente alcuni programmi senza passare per il menu Start oppure a dare informazioni sullo stato del computer.

Considerato che lo scopo di queste icone è offrirvi un accesso rapido a programmi e informazioni, è piuttosto ridicolo che Windows faccia di tutto per nascondervele quando (a suo parere) non le usate abbastanza.

Se volete impedirgli di essere così erroneamente servizievole, cliccate con il pulsante destro del mouse in una zona vuota della barra delle applicazioni (non su un pulsante di un'applicazione aperta) e scegliete *Proprietà* (Figura 3.10). Nella scheda *Barra delle applicazioni*, rimuovete il segno di spunta da *Nascondi icone inattive* e cliccate su *OK*.

Figura 3.10

Rivoglio i miei pulsanti!

Già che siamo in ballo con le modifiche al comportamento di Windows, se volete tornare alla barra delle applicazioni "vecchia maniera" (con un pulsante per ogni finestra di applicazione, invece che con un pulsante per ogni raggruppamento di finestre affini), in

modo da ridurre le cliccate necessarie per raggiungere un'applicazione, potete procedere come segue:

- cliccate con il pulsante destro del mouse in una zona vuota della barra delle applicazioni;
- scegliete *Proprietà* e cliccate, nella scheda *Barra delle applicazioni*, su *Raggruppa pulsanti* in modo da rimuovere il segno di spunta;
- cliccate su OK e il gioco è fatto.

Infine, se volete la massima comodità nel personalizzare il menu Start:

- cliccate con il pulsante destro del mouse sul pulsante Start e scegliete *Esplora* (oppure *Esplora cartella utenti* se volete apportare le stesse modifiche a tutti gli utenti del computer);
- si apre una finestra di Esplora risorse che elenca le voci del menu Start, da spostare e manipolare esattamente come fareste con un qualsiasi file (infatti *sono* dei file).

Finalmente si comincia a ragionare. Avete dissipato buona parte della cortina fumogena che i maghi dell'estetica avevano eretto per far sembrare Windows più "bello". Sbarazzarsene del tutto è impossibile, ma quello che avete fatto fin qui è un ottimo passo avanti verso la trasparenza e il controllo del vostro computer.

Capitolo 4

Turiamo qualche falla?

Non sentitevi in obbligo di seguire subito per filo e per segno i consigli di questo capitolo: sono alcuni esempi di falle di Windows XP con le relative soluzioni, giusto per farvi capire che non sto esagerando a proposito della facilità con la quale si devasta o si invade un computer Windows. Prima o poi, però, ricordatevi di tornare qui e turare queste falle, magari con l'aiuto di un amico o collega esperto.

A proposito: scusatemi per l'involontario maschilismo implicito nella grammatica italiana, ma sia ben chiaro che qui e altrove, quando dico *"amico o collega"*, includo naturalmente anche il gentil sesso.

Infili il CD, infetti il PC

Uno dei modi più semplici per infettare Windows o iniettargli programmi-spia è usare la funzione di esecuzione automatica dei CD e DVD di programmi appena vengono inseriti nel lettore, denominata *Autorun*.

Può sembrare utile che Windows esegua automaticamente i CD/DVD contenenti programmi: così dovete soltanto infilare il disco di installazione nel lettore e Windows, bontà sua, fa tutto da solo.

Il guaio è che questo automatismo viene sfruttato con entusiasmo dagli aggressori: infatti l'Autorun esegue ciecamente qualsiasi istruzione specificata in un apposito file, *autorun.inf* (notate l'estensione pericolosa *.inf*), presente sul disco che inserite nel lettore.

> *L'Autorun è usato principalmente per CD e DVD, ma funziona anche con qualsiasi supporto collegabile alla porta USB, per esempio una di quelle praticissime memorie tascabili allo stato solido, che si comportano come un disco rigido e stanno ormai soppiantando i dischetti.*

Se il file *autorun.inf* contiene l'istruzione *"installa un virus"*, Windows è così premuroso da ubbidire automaticamente. Questo consente a un vandalo di avvicinarsi a un PC, infilare un CD o DVD appositamente confezionato e devastare il computer (o prenderne segretamente il controllo) in una manciata di secondi.

Non è necessario, tuttavia, che il vandalo vi entri in casa. Molti CD/DVD di software copiato illegalmente contengono veri e propri "cavalli di Troia" (*Trojan horse*): promettono di regalarvi copie scroccate di programmi costosi, ma nel frattempo vi infettano il computer usando questa funzione di esecuzione automatica. Ci sono molti altri modi per infettarvi di nascosto, ma questo è uno dei più semplici ed efficaci.

Questo è un tipico esempio di come sicurezza e facilità d'uso spesso diventano obiettivi contrastanti, se non vengono progettati con saggezza, e dimostra come Microsoft troppo spesso introduce facilità a discapito della sicurezza. Per evitare all'utente la tremenda fatica di cliccare un paio di volte in Esplora Risorse, la casa produttrice di Windows ha deciso di esporlo a un pericolo.

Rimedi anti-automatismi

Disattivare *temporaneamente* questa funzione pericolosa è molto semplice: basta premere il tasto Shift (Maiusc) mentre si inserisce il CD/DVD.[21] Disabilitarla permanentemente è un po' più impegnativo. Ci sono vari modi per farlo,[22] ma il più semplice è ricorrere al programma *TweakUI* (si legge, che ci crediate o no, *"tuik-iu-ai"*), scaricabile gratuitamente dal sito Microsoft presso *www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx*.

Microsoft fornisce TweakUI senza garanzie e con la precisazione[23] che funziona soltanto con Windows XP impostato per l'inglese americano, ma nei miei test ha funzionato egregiamente anche nella versione italiana di XP, perlomeno per quanto riguarda disattivare l'esecuzione automatica dei supporti rimovibili.

Per installare TweakUI è sufficiente eseguire il programma omonimo scaricato dal sito Microsoft. A installazione completata, trovate TweakUI in Start > Programmi > Powertoys for Windows XP > TweakUI. Lanciatelo e andate alla sezione My computer > AutoPlay > Types (purtroppo TweakUI parla soltanto inglese).

Disattivate *Enable Autoplay for CD and DVD drives* e *Enable Autoplay for removable drives,* poi cliccate su OK. Non occorre riavviare il computer perché la modifica abbia effetto.

A questo punto, se inserite un CD/DVD o altro supporto rimovibile contenente un file *autorun.inf*, non verrà eseguito automaticamente; inoltre i supporti contenenti immagini non verranno aperti automaticamente.

Se preferite un approccio da "veri smanettoni", senza dover installare un programma, c'è un metodo più diretto ma più delicato, nel senso che se sbagliate, rischiate di rendere inservibile Windows: per questo l'ho relegato nel capitolo supplementare *Per veri smanettoni* che trovate presso *www.attivissimo.net.* Se volete, potete chiedere a un amico esperto di eseguire questo metodo per voi (dopo avergli promesso l'immunità in caso di pasticci).

> *L'aggiornamento di Windows denominato Service Pack 2, descritto in dettaglio nei capitoli successivi, disattiva l'automatismo di questa funzione, visualizzando invece una finestra di dialogo che chiede ogni volta cosa volete fare.*

E adesso come installo?

Bella furbata, direte voi, e adesso che ho spento l'automatismo come faccio a usare i CD/DVD autoinstallanti?

Semplice: li inserite (ovviamente soltanto se sono di provenienza affidabile), usate Esplora Risorse per elencarne la cartella principale, fate doppio clic sul file *autorun.inf* per aprirlo nel Blocco Note (dunque senza eseguirlo) e guardate il nome del file che compare dopo la parola *open*. Trovate quel file nella cartella principale del CD/DVD e lanciatelo con il consueto doppio clic.

Scomodo? È il prezzo da pagare per una maggiore sicurezza. Trovarsi il computer infettato è molto più scomodo, ve lo assicuro. Chiedete a qualcuno a cui è capitato.

Questa modifica, fra l'altro, blocca anche l'esecuzione automatica di dischi o altri supporti contenenti musica, immagini o video, che non è un vero rischio per la sicurezza ma spesso si rivela una scocciatura. Accendere il computer la sera tardi e sentir partire i Metallica a tutto volume perché avete dimenticato il loro CD nel

PC può causare un giustificato lancio di oggetti da parte dei presenti.[24]

Strani messaggi sullo schermo

Mentre siete collegati a Internet, anche se non state navigando nel Web, possono comparirvi sullo schermo degli strani messaggi, come quello mostrato nella Figura 4.1.[25]

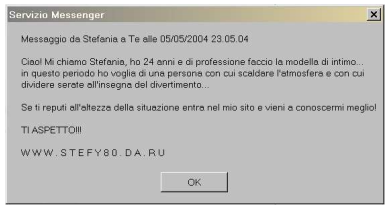

Figura 4.1

Si chiamano *Messenger spam*: sono una forma di intrusione pubblicitaria nel vostro computer. Non fanno danni diretti, anche se possono causare confusione e allarme inutile quando simulano di essere un avviso di sicurezza di Windows, oppure fastidio e imbarazzo quando il loro messaggio è a contenuto pornografico.

Il nome deriva dalla combinazione di *Messenger*, che è il servizio di Windows incaricato di visualizzare messaggi riguardanti lo stato del computer o comunicazioni di altri utenti della rete locale, con *spam*, che è il nome usato per indicare la pubblicità indesiderata di Internet. Il servizio Messenger non va confuso con *MSN Messenger*, un popolare programma di *chat*.

In sostanza, nel Messenger spam un pubblicitario senza scrupoli manda al vostro computer un comando che gli ordina di visualizzare una finestra informativa, il cui contenuto è il testo della pubblicità.

Fra l'altro, il servizio Messenger è colpevole di una vulnerabilità anche peggiore, che consente a un aggressore di prendere il controllo del vostro computer via Internet.[26]

Per eliminare queste falle potete disattivare il servizio Messenger come segue:

- Dal menu Start, scegliete *Impostazioni* > *Pannello di controllo* > *Strumenti di amministrazione* > *Servizi*.
- Fate doppio clic su *Messenger* e selezionate *Disabilitato* da *Tipo di avvio*.
- Cliccate su *OK* e poi di nuovo su *OK*.

Per maggiore sicurezza, vi conviene installare inoltre la correzione appositamente fornita da Microsoft, come spiegato nel capitolo intitolato *Mettiamoci una pezza*.

In alternativa, se ve la cavate con l'inglese potete usare il programma gratuito *Shoot the Messenger*, disponibile presso il sito *Grc.com*.

> *Il Service Pack 2 di Windows XP disabilita automaticamente Messenger e risolve il problema alla radice.*

Clicchi nel Web, si cancella tutto Windows

Un'altra delle più spettacolari vulnerabilità di un'installazione di Windows XP non aggiornata consente a un aggressore di confezionare un e-mail o una pagina Web nella quale basta cliccare su un *link* (collegamento o rimando) apparentemente innocuo per cancellare qualsiasi file del computer, a scelta dell'aggressore.[27]

La falla è facilmente verificabile nel test numero 7 del *Browser Challenge*, che è una piccola serie di prove innocue, disponibile presso il mio sito ***www.attivissimo.net***. Vi consiglio di eseguirle tutte; è un'esperienza illuminante per capire quanti difetti ci sono nei programmi comunemente utilizzati.

Ci sono vari modi per turare questa falla, se la vostra sottoversione di Windows è vulnerabile:

- non usare Internet Explorer, perlomeno nei siti a rischio (argomento che approfondirò nei prossimi capitoli);
- installare gli aggiornamenti gratuiti di Windows XP, come descritto nel capitolo *Mettiamoci una pezza*;

- cancellare o rinominare il file *updrvinfo.htm* dalla sottocartella *pchealth\helpctr\system\dfs* della cartella di Windows (di solito *c:\windows*).[28]

Dopo la modifica, il test del *Browser Challenge* deve fallire.

"Sottoversioni"?

Se vi state chiedendo che cos'è una *sottoversione* di Windows, mi spiego subito. Tutti conosciamo le *versioni* o *edizioni* di Windows, quelle chiamate Windows 3.1, Windows 95, Windows 98, Windows ME, Windows XP, Windows 2000 e così via; sono quelle ampiamente pubblicizzate da Microsoft.

Microsoft, tuttavia, non se ne sta con le mani in mano fra una versione e l'altra. Corregge magagne e introduce migliorie, includendole senza squilli di tromba nei Windows preinstallati venduti insieme ai computer e in quelli acquistabili a parte.

Di conseguenza, il Windows XP che avreste trovato preinstallato in un computer del 2002 è assai diverso dal Windows XP che ricevete preinstallato in un computer acquistato oggi. Questi "gemelli diversi" sono le *sottoversioni*.

Per sapere quale sottoversione di Windows XP avete, andate in Esplora risorse, scegliete la Guida e la voce *Informazioni su Windows*, oppure cliccate con il pulsante destro del mouse sull'icona di Risorse del computer e scegliete *Proprietà* e poi la scheda *Generale*.

Disattivare il controllo remoto

Windows XP ha un'opzione che consente a un tecnico di farvi assistenza a distanza: lasciate il computer connesso a Internet, attivate l'opzione di assistenza remota e il tecnico vi entra nel computer e lo sistema a puntino.

Molto comodo. Ma che succede se al posto del tecnico entra un malintenzionato?

È assolutamente irresponsabile e inutile tenere continuamente attivata questa funzione: è un invito a nozze per qualsiasi aggressore. Non sono note al momento vulnerabilità che la sfruttano, ma il buon senso suggerisce che comunque è poco prudente lasciarla

attiva quando non serve. È molto più saggio attivarla all'occorrenza.

Per fare un paragone pratico: affidereste permanentemente una copia delle chiavi di casa al riparatore della vostra lavatrice, così non deve disturbarvi quando occorre il suo intervento e può entrare da solo quando gli pare? O preferireste tenervi le chiavi e aspettarlo in casa? Appunto.

Per disattivare il controllo remoto:

- Nel menu Start, scegliete *Impostazioni* > *Pannello di controllo* > *Sistema* e la scheda *Connessione remota*.
- Cliccate su *Avanzate* e disattivate *Consenti il controllo del computer da postazioni remote*. Confermate cliccando su OK.
- Disattivate *Consenti invio inviti di Assistenza remota da questo computer* e confermate cliccando su OK.

Altri servizi inutili e/o pericolosi

Windows XP contiene un vasto assortimento di cosiddetti *servizi*. Niente a che fare con i gabinetti: si tratta di programmi automatici che gestiscono dietro le quinte numerose funzioni di amministrazione e manutenzione del computer.

Il guaio è che gran parte di questi servizi, nelle normali circostanze d'uso del computer, è superflua e appesantisce inutilmente il funzionamento di Windows, occupando decine e decine di megabyte di memoria RAM e rallentando l'avvio del PC.

Al tempo stesso, questi servizi possono offrire appigli agli aggressori e rivelare informazioni private su di voi. Insomma, se non vi servono, è opportuno disattivarli.

Nel menu Start, scegliete *Impostazioni* > *Pannello di controllo* > *Strumenti di amministrazione* > *Servizi*. Fate doppio clic su ciascuna delle seguenti voci e selezionate *Disabilitato* da *Tipo di avvio,* se non lo è già:

- *Clipbook*
- *Condivisione desktop remoto di NetMeeting*
- *Gestione sessione di assistenza mediante desktop remoto*

- *Host di periferiche Plug and Play universali*
- *Numero di serie del supporto portatile* (dopo l'installazione del Service Pack 2, diventa *Servizio Numero di serie per dispositivi multimediali portatili*)
- *Routing e Accesso remoto*
- *Servizio di rilevamento SSDP*
- *Servizio di segnalazione errori*
- *Utilità di pianificazione* (a meno che vogliate che l'antivirus effettui scansioni e aggiornamenti in modo automatico)[29]
- *Zero Configuration reti senza fili*

Al termine cliccate su *OK*.

Questo è un elenco molto parziale e prudenziale di servizi superflui e potenzialmente pericolosi: ce ne sono molti altri probabilmente disattivabili nella vostra specifica situazione, ma per ora vi conviene limitarvi a questi. Quando sarete più pratici di queste cose potrete snidare i servizi inutili restanti.[30]

Una strada piena di buche

In questo capitolo avete fatto conoscenza con una piccola dose di vulnerabilità di Windows. Probabilmente a questo punto state cominciando a rendervi conto che la definizione di *"colabrodo"* non era poi così immeritata. Coraggio, il peggio deve ancora venire.

Ma alla fine ne emergerete vittoriosi, più sani e più sicuri di prima.

Capitolo 5

Firewall: il buttafuori digitale

La prima linea di difesa

Ho scelto di cominciare il lavoro di blindatura partendo da questo strumento di difesa dal nome piuttosto arcano perché Windows XP ha un problema fondamentale: così com'è, **può essere sufficiente collegarlo a Internet per infettarlo**. Ed è ovviamente inutile lavorare alla protezione del computer se il nemico è già dentro le mura. Ecco perché la prima regola del Dodecalogo parla di firewall:

> ***Regola 1: Installate un buon firewall.***

Cos'è un firewall? E soprattutto, come cavolo si pronuncia?

Un firewall è l'equivalente informatico di un buttafuori. È un programma, residente nel vostro computer o in un apparecchio esterno, che respinge le visite indesiderate e fa entrare e uscire soltanto i dati che autorizzate a circolare. E là fuori, su Internet, ci sono tanti individui e virus indesiderati e indesiderabili.

E visto che me lo chiedete, si pronuncia *"faier-uool"*. Beh, più o meno; accontentatevi. Ricordate inoltre che *firewall* significa *"parete tagliafuoco"*, non *"muro di fuoco"* come scrivono certi giornalisti figli di papà.

> ***Navigare in Internet con Windows senza firewall significa cercarsi guai.***
>
> ***Windows XP è dotato di un firewall, ma è normalmente disattivato*** *(viene attivato automaticamente soltanto se avete l'aggiornamento chiamato* Service Pack 2*). Il che è profondamente stupido, come installare una porta blindata in casa e non chiuderla mai a chiave, ma tant'è.*

Se non avete il Service Pack 2, non perdete tempo ad attivare il firewall integrato in Windows: *per ammissione della stessa Microsoft, la versione pre-Service Pack 2 è un colabrodo*[31] *e comunque non blocca il traffico* uscente *dal vostro computer, per cui un virus che vi infetta può lanciare attacchi dal vostro PC verso altri utenti sotto il naso del firewall Microsoft.*

Le cose migliorano leggermente se usate il firewall aggiornato presente nel Service Pack 2, come descritto a fine capitolo.

Installare un firewall è un'esperienza rivelatrice. Potreste pensare che non vi serva, perché tanto non vi capita mai di essere attaccati: non avete nemici così ostili. La realtà è ben diversa: siamo *tutti* sotto attacco quasi continuamente, solo che non ce ne accorgiamo perché Windows, come molti altri sistemi operativi, preferisce non farcelo vedere. Non ha tutti i torti: occhio non vede, cuore non duole.

Virus e vandali della Rete, infatti, tentano a casaccio di accedere a *tutti* i computer che trovano connessi a Internet. Niente di personale, insomma: è un procedimento casuale. Chi capita, capita. Il firewall rivela questo brulichio incessante di tentativi d'accesso e il primo impatto è scioccante.

Tuttavia lo stupore iniziale di vedersi sotto continua aggressione diventa molto presto scocciatura, per cui di solito si disattivano le notifiche (ma non l'efficacia) del firewall, in modo che ci protegga silenziosamente, senza disturbarci ogni volta per dirci *"Ehi! Ho bloccato un altro intruso! Come sono bravo!!"*.

La sorpresa successiva nasce quando ci si accorge di quanti dei nostri normalissimi programmi tentano di *uscire* dal nostro computer, anche se apparentemente non hanno ragione di farlo.

- Windows Media Player, per esempio, tenta spesso di uscire quando vediamo un filmato o ascoltiamo una canzone presente nel nostro computer.
- Quando chiediamo alla funzione di ricerca file di Esplora Risorse di cercare un file sul nostro disco rigido, la prima cosa che fa Esplora Risorse è tentare di andare su Internet.

- Lo fa spesso anche Acrobat Reader, il programma che si usa per leggere i diffusissimi documenti in formato PDF.
- La lista potrebbe continuare a lungo: ho colto in flagrante sia Word, sia programmi alternativi come OpenOffice.org[32], sia programmi di elaborazione audio come SoundForge. Non è un vezzo esclusivo di Microsoft, insomma.

Perché vogliono uscire? Con chi vogliono comunicare, e cosa vogliono dirgli? Non so voi, ma l'idea che ci siano queste comunicazioni a mia insaputa non mi lascia tranquillo. Nel dubbio, è meglio impedirle o perlomeno esserne informati.

Sorvegliare il traffico *uscente* è importante anche per un'altra ragione. Molti virus si insediano nel computer senza fare danno apparente ma *"zombificandolo"*, ossia trasformandolo in uno schiavo che ubbidisce segretamente agli ordini del suo misterioso padrone (che spesso è uno *spammer* o un altro tipo di truffatore).

Una volta insediati, questi virus devono comunicare con il proprio padrone e tentare di trasmettersi ad altri utenti. Un firewall decente si deve accorgere di questi tentativi di comunicazione da parte di un programma non autorizzato e bloccarli. In altre parole, il firewall deve impedire che l'infezione che vi ha colpito si possa estendere ad altri utenti.

Il problema è assai meno raro di quel che potreste pensare: le società del settore informatico stimano che almeno un terzo della posta-spazzatura (lo *spam*) è generata da computer "zombificati".[33]

Ma perché mi serve un firewall? Ho già l'antivirus!

La sicurezza non si ottiene mai mediante una singola soluzione; si conquista combinando vari ingredienti. È un po' come mettere la cintura e anche le bretelle: un po' scomodo, ma riduce moltissimo le probabilità di trovarsi con le braghe calate nel momento meno opportuno se cede uno dei due supporti.

A parte questo, il firewall agisce contro pericoli diversi da quelli sorvegliati da un antivirus. L'antivirus ci difende contro i *file* ostili recapitati al nostro computer; il firewall ci protegge dalle *intrusioni* perpetrate direttamente via Internet o tramite la rete locale.

Per esempio, se un e-mail contiene un allegato infetto, il firewall lo lascerà passare, perché dal suo punto di vista si tratta di traffico di dati legittimo; sta poi all'antivirus determinare che l'allegato è pericoloso. Per contro, se un aggressore tenta di far leva su una falla di Windows o di un nostro programma per penetrare le nostre difese, l'antivirus non se ne accorgerà, ma il firewall sì.

Fra le due forme di attacco c'è comunque oggigiorno una certa sovrapposizione: per esempio, certi firewall bloccano anche alcuni tipi di virus e alcuni antivirus fermano gli intrusi che cercano di farci visitare una pagina Web infetta. Tuttavia, grosso modo la suddivisione dei compiti è questa: bloccare i file ostili spetta all'antivirus, fermare gli attacchi diretti è compito del firewall.

Come funziona un firewall

Il firewall è un programma perennemente attivo, che osserva tutto il traffico di dati che entra ed esce tramite le connessioni di rete (connessioni alla rete locale e connessioni a Internet di qualunque tipo). Quando rileva traffico di tipo anomalo o sospetto, lo segnala all'utente oppure lo blocca direttamente.

Per quanto riguarda il traffico uscente, la maggior parte dei firewall è in grado di capire quale programma lo sta generando e comportarsi di conseguenza. Per esempio, per inviare un e-mail è abbastanza ovvio che il vostro programma di posta deve trasmettere dei dati verso Internet; il firewall riconosce il programma che genera la trasmissione e (con il vostro preventivo consenso) gli permette di effettuarla.

Il firewall esamina anche il traffico ricevuto dalla rete locale o da Internet e riconosce e blocca quello ostile, lasciando passare invece quello sicuro. Per esempio, per scaricare la posta dovete evidentemente ricevere dati da Internet: il firewall riconosce che si tratta di e-mail e lascia passare. Se invece un vandalo cerca di entrare nel vostro computer, il firewall rileva i dati ostili mandati dall'aggressore e li blocca.

Un firewall permette anche di essere selettivi nell'accettare comunicazioni da altri computer. Normalmente un computer accetta trasmissioni di dati da qualunque altro computer della rete locale o di Internet, ma questo significa che le accetta anche dagli utenti ostili. Il firewall consente di creare una "lista nera" di computer indesi-

derati oppure una "lista bianca" che specifica gli unici computer dai quali si accettano comunicazioni.

Alcuni firewall usano la *modalità di occultamento* (*stealth mode* in gergo): in sostanza, rendono invisibile su Internet il vostro computer, in modo tale che l'aggressore medio non si accorga affatto della vostra esistenza e quindi non pensi neppure di prendervi di mira. Un aggressore esperto sa accorgersi di questo trucco, ma se non ce l'ha specificamente con voi, vi lascerà comunque stare e andrà a cercarsi bersagli meno protetti. Tanto Internet è piena di prede facili.

Come agisce un aggressore

Per capire quanto sia importante e utile un firewall bisogna conoscere un pochino la psicologia degli aggressori informatici e il loro modo di operare.

Come già accennato, se non siete individui particolarmente in vista o non vi siete fatti troppi nemici, è difficile che un attacco vi prenda di mira personalmente. L'aggressore medio non fa altro che gironzolare per Internet alla ricerca di qualche preda, quasi sempre senza curarsi di chi sia la persona che aggredisce.

Come un predatore nella savana, prende di mira preferibilmente i soggetti più deboli e vulnerabili, lasciando perdere quelli meglio difesi o così ben mimetizzati da sfuggire alla sua perlustrazione.

È un paragone molto poetico, perlomeno per le mie capacità letterarie, ma all'atto pratico come funziona la cosa? A ogni computer collegato a Internet viene assegnato un *indirizzo* permanente o temporaneo, chiamato *indirizzo IP* e solitamente espresso sotto forma di quattro numeri in serie, per esempio *212.162.1.47*. È grosso modo paragonabile al numero telefonico assegnato al vostro cellulare.

Usando appositi programmi, l'aggressore "chiama" tutti gli indirizzi compresi in una certa gamma e vede chi risponde, esattamente come un molestatore telefonico può comporre una rosa di numeri a caso alla ricerca di una vittima dalla voce promettente.

Se l'aggressore trova un indirizzo che gli risponde, passa alla seconda fase dell'attacco: trovare un varco. Per gestire il traffico di dati, ogni computer collegato a Internet suddivide la connessione

in *porte* (non sono oggetti reali come le porte USB alle quali collegate una stampante, ma delle convenzioni virtuali). La posta inviata passa da una determinata porta, quella ricevuta entra da un'altra, le pagine Web arrivano da un'altra ancora e così via. Per ogni servizio di Internet c'è una porta corrispondente (o più d'una).

L'aggressore "bussa" a ciascuna di queste porte per vedere se per caso dall'altra parte c'è una risposta e controlla se la porta è chiusa a chiave o aperta. La risposta può provenire per esempio da un virus precedentemente insediatosi, da un programma volutamente installato nel PC (per esempio uno di quelli usati per scambiare musica) o da un errore di impostazione del sistema operativo. In tutti i casi, l'aggressore può usare questa risposta come appiglio per tentare di far danni.

Una delle tecniche di attacco più diffuse è inviare dati in formati anomali. I programmi e le funzioni di Windows che stanno in ascolto sulle porte sono spesso ingenui e si aspettano che i dati in arrivo rispettino le convenzioni, andando invece in tilt (e permettendo all'aggressore di devastare il computer) se i dati sono confezionati in modo appositamente anomalo.

Lo scopo del firewall è prevenire tutto questo. Innanzitutto, il firewall "chiude a chiave" tutte le porte lasciate incautamente aperte dai programmi e da Windows e rifiuta di rispondere a chi "bussa" da fuori, in modo da non offrire appigli: fa finta che in casa non ci sia nessuno, come si fa con i venditori porta a porta.

Successivamente, il firewall previene l'aggressione nascondendo l'esistenza del vostro computer con un semplice espediente: quando un aggressore bussa al vostro indirizzo IP, il firewall non solo non gli risponde, ma gli fa credere che quell'indirizzo non sia assegnato.

Per tornare al paragone telefonico, è come se il molestatore componesse il vostro numero di telefono e invece di sentire il tono di libero, sentisse la voce della Telecom che annuncia che il numero chiamato è inesistente. In entrambi i casi, il rompiscatole desisterà e andrà a cercare altrove.

È per questo che siamo tutti sotto attacco ripetutamente nell'arco della giornata e dobbiamo difenderci con un firewall. Là fuori ci sono migliaia di vandali sfigati che si sfogano cercando computer vulnerabili e bussando alle loro porte in cerca di qualche pertugio

dal quale intrufolarsi per fare danni o spiare. A loro non interessa chi siete: interessa soltanto trovare un bersaglio facile.

Scegliere un firewall

Esistono due grandi famiglie di firewall: quelli *software*, ossia costituiti da programmi-sentinella da installare nel computer, e quelli *hardware*, vale a dire apparecchi autonomi e separati dal computer, che contengono un programma-sentinella.

I **firewall hardware** sono molto più efficaci di quelli software, perché sono apparecchi indipendenti e quindi immuni alle falle di Windows, ma sono anche più costosi. Se potete, investite in un firewall hardware, specialmente se dovete proteggere più di un computer (ne basta uno per tutti i computer). È quello che fanno tutte le aziende che hanno un minimo di riguardo per la sicurezza.[34]

Talvolta il firewall hardware è integrato nell'apparecchio che usate per collegarvi a Internet, specialmente nel caso di connessioni ADSL. Date un'occhiata al manuale del vostro modem ADSL: può darsi che contenga un firewall e non lo sappiate. In tal caso, siete già a posto.

Se non potete permettervi la spesa di un firewall hardware, potete ricorrere a un **firewall software**. Ve ne sono molti gratuiti che funzionano benissimo; se volete maggiore versatilità e assistenza tecnica, potete rivolgervi ai firewall a pagamento. In questo capitolo vi presenterò soltanto i firewall software, perché sono la soluzione di gran lunga più diffusa.

Tenete presente, comunque, che esistono tecniche di intrusione che permettono di spegnere a distanza un firewall software, se l'utente abbocca all'esca; è molto più difficile spegnere un firewall hardware.

> *Se vi state chiedendo come scaricare un firewall software, visto che per scaricarlo bisogna collegarsi a Internet ma vi ho sconsigliato di collegarvi a Internet senza firewall, il trucco è semplice: chiedete a qualcun altro di scaricarlo con il* suo *computer già protetto e di darvi il firewall su un CD*.

La strana coppia

Nulla vieta di abbinare un firewall hardware e uno software, per esempio quello integrato nel vostro modem ADSL e uno installato sul PC. I firewall hardware, infatti, solitamente bloccano i tentativi di aggressione in entrata, ma non fanno molto contro quelli in uscita; molti firewall software, invece, sorvegliano i tentativi ostili anche in uscita.

Un firewall hardware a guardia della connessione a Internet e uno sul PC sono una buona coppia anche nel caso di una rete locale di computer (per esempio in ufficio). Il primo protegge il perimetro, per così dire, mentre il secondo evita che un'eventuale contaminazione di un computer possa diffondersi agli altri. È come mettere un buttafuori all'ingresso principale e altri nerboruti sorveglianti alle porte dei singoli uffici.

L'inconveniente principale di un doppio firewall misto è che se qualcosa non funziona nella comunicazione verso Internet, è più difficile determinarne la causa, perché bisogna scoprire quale dei due firewall la sta bloccando (per esempio disabilitando il firewall software e guardando se questo risolve il problema). Nel caso di una rete locale, possono inoltre sorgere difficoltà nella condivisione di file e stampanti se il firewall software non è impostato correttamente per consentirla.

Firewall a scelta

Ecco una breve rassegna dei più gettonati firewall software.

- **Nome:** BlackICE PC Protection
  Produttore e sito: Internet Security Systems, *blackice.iss.net/product_pc_protection.php*
  Prezzo: a pagamento
  Lingua: inglese
- **Nome:** Conseal Firewall/8signs Firewall
  Produttore e sito: 8signs, *www.consealfirewall.com*
  Prezzo: a pagamento, versione dimostrativa scaricabile gratis
  Lingua: inglese
- **Nome:** F-Secure Internet Security
  Produttore e sito: F-Secure, *www.f-secure.it*
  Prezzo: a pagamento; versione dimostrativa scaricabile gratis
  Lingua: italiano

- **Nome:** Kerio Personal Firewall
  Produttore e sito: Kerio, *www.kerio.com*
  Prezzo: la versione *Limited Free Edition* è gratuita per uso personale
  Lingua: inglese
- **Nome:** McAfee Personal Firewall Plus
  Produttore e sito: McAfee, *it.mcafee.com*
  Prezzo: a pagamento
  Lingua: italiano
- **Nome:** Norton Personal Firewall
  Produttore e sito: Symantec, *www.symantec.it/region/it/product/npf_index.-html*
  Prezzo: a pagamento
  Lingua: italiano
- **Nome:** Outpost Firewall Pro
  Produttore e sito: Agnitum, *www.agnitum.it*
  Prezzo: a pagamento; versione dimostrativa scaricabile
  Lingua: italiano
- **Nome:** Panda Platinum Internet Security
  Produttore e sito: Panda Software, *us.pandasoftware.com/com/it/*
  Prezzo: a pagamento
  Lingua: italiano
- **Nome:** Sygate Personal Firewall
  Produttore e sito: Sygate, *smb.sygate.com/products/spf_standard.htm*
  Prezzo: gratuito per uso personale; la versione Pro è a pagamento
  Lingua: inglese
- **Nome:** Tiny Personal Firewall
  Produttore e sito: Tiny, *www.tinysoftware.com/home/tiny2?la=IT*
  Prezzo: a pagamento
  Lingua: inglese
- **Nome:** Zone Alarm
  Produttore e sito: Zone Labs, *www.zonelabs.com*
  Prezzo: gratuito per uso personale; la versione Plus/Pro è a pagamento
  Lingua: inglese, francese, tedesco, spagnolo, giapponese

Sul mio sito www.attivissimo.net, *nella sezione dedicata a questo libro, trovate le istruzioni dettagliate per scaricare, installare e configurare la versione gratuita di Zone Alarm. Anche se scegliete di non usare questo firewall,*

leggetele comunque: i principi presentati sono validi per quasi tutti i firewall.

Configurare un firewall

Molti pensano che configurare un firewall sia un'impresa complicatissima e che i firewall siano grandi scocciatori che gridano continuamente *"al lupo, al lupo"* senza motivo, causando falsi allarmi e intralciando l'uso del computer.

A causa di questi preconcetti, capita che gli utenti si rifiutino di installare un firewall. Poi piangono quando arrivano virus come Blaster, Sasser e compagnia bella, che si infilano automaticamente nel computer sfruttando un difetto di Windows che qualsiasi firewall è in grado di compensare.

In realtà tutto dipende dal firewall che si sceglie e da come lo si configura. L'errore che si commette spesso è lasciare attivate le notifiche dei tentativi di intrusione. A prima vista questo può sembrare il modo giusto di procedere, ma in realtà i tentativi sono talmente frequenti che **ciò che conta non è esserne informati, ma esserne protetti.**

Il firewall va insomma configurato in modo che agisca silenziosamente e automaticamente contro le minacce provenienti dall'esterno, così come un buttafuori non va a riferire in continuazione al capo quando si sbarazza di un avventore molesto.

Salvo casi rari, inoltre, cercare di scoprire chi sta dietro i tanti tentativi di penetrazione è soltanto una perdita di tempo: principalmente per ragioni legali, le possibilità di ricavarne informazioni che possano portare a una punizione del colpevole sono irrisorie. Anche in questo caso, insomma, è importante la protezione più che l'informazione.

Avvisi e permessi

La vera difficoltà nell'uso di un firewall sta nel saper rispondere agli allarmi generati dai programmi che tentano di uscire, soprattutto nel periodo iniziale d'uso del nostro buttafuori digitale, quando deve ancora imparare a conoscere i programmi fidati.

Anche in questo caso, comunque, basta applicare un criterio di base abbastanza semplice:

> *Se un programma chiede di andare su Internet o accedere alla rete locale, chiedetevi perché. Se non c'è un motivo più che valido, non importa che programma è, glielo si deve vietare. Nel dubbio, non autorizzate. Potete sempre autorizzarlo in seguito se vi accorgete che vi serve ed è innocuo.*

In altre parole, se non siete veramente sicuri di cosa fa un certo programma che chiede l'autorizzazione, non autorizzatelo; dategli il permesso soltanto se non darglielo rende impossibile usare Internet.

> *Sul mio sito* www.attivissimo.net, *nella sezione* Acchiappavirus*, trovate un elenco dei nomi dei programmi più frequentemente rilevati dai firewall, con i relativi consigli di autorizzazione o blocco.*

Tenete sempre presente che i vandali della Rete non aspettano altro che un vostro passo falso. Concedete quindi le autorizzazioni con estrema parsimonia.

Come si fa a sapere se un programma è fidato o no? Vi conviene partire dal presupposto che ciò che non conoscete è malvagio fino a prova contraria, per cui cominciate a vietarne l'uscita temporaneamente; nel frattempo, indagate immettendo il nome del programma in Google o chiedendo a un amico o collega esperto.

Molto spesso i programmi che tentano di uscire sono componenti legittimi di Windows, con nomi come per esempio *svchost.exe*, *spoolsv.exe*, *jucheck.exe, explorer.exe, cmd.exe, rundll.exe*, oppure sono componenti dell'antivirus che cercano di uscire per scaricare i propri aggiornamenti.

In tal caso, dopo aver appurato che si tratta effettivamente di programmi regolari, vi conviene autorizzarli (meglio se in modo non permanente, così ne tenete sotto controllo l'attività).

> *Nel caso di questi componenti legittimi è estremamente importante tenere d'occhio le segnalazioni del firewall. I vandali astuti, infatti, tentano di mascherare i propri programmi-trappola dando loro nomi simili a quelli di questi componenti (per esempio* svchosts.exe *al posto di* sv-

chost.exe*) oppure sostituendo direttamente il componente legittimo con uno ostile omonimo.*

Internet Explorer, sorvegliato speciale

Nella scelta di cosa autorizzare e cosa vietare, Internet Explorer (*iexplore.exe*) è un caso un po' particolare. L'abitudine e l'istinto probabilmente vi suggeriscono di dargli un'autorizzazione permanente, visto che lo usate spessissimo, ma permettetemi di sconsigliarvelo in favore di un'autorizzazione di volta in volta.

Internet Explorer, il programma Microsoft per la navigazione nel Web, è infatti uno dei principali veicoli di infezione degli aggressori. **Visualizzare un sito ostile con Internet Explorer può essere sufficiente per contaminare e devastare il vostro computer.** È un problema così serio che il CERT, ente del Dipartimento per la Sicurezza Interna USA, ad agosto 2004 è arrivato al punto di sconsigliare l'uso di Internet Explorer, raccomandando di sostituirlo con programmi di navigazione (*browser*) alternativi.[35]

Per questo la navigazione con Internet Explorer va ridotta al minimo indispensabile, usando al suo posto un programma alternativo, come descritto nei capitoli successivi.

Ci sono però parecchi siti che per ragioni particolarmente stupide funzionano soltanto con Internet Explorer, alla faccia dell'universalità di Internet (è come aprire un negozio di vestiti che fa entrare soltanto clienti di taglia media e lascia sulla porta tutti gli altri). Sono siti che magari non potete ignorare, come quelli di banche o istituzioni governative; è un numero in rapida diminuzione, dopo gli spaventi causati dalle falle passate di Internet Explorer, ma comunque non trascurabile.

Se vi imbattete in uno di questi siti, potete tirar fuori Internet Explorer e fargli fare un giretto, ma mi raccomando: usatelo soltanto su siti di reputazione più che cristallina.

*Ricordate comunque che **il firewall da solo non basta:** deve far parte di un **insieme** di contromisure difensive che vedremo nei capitoli successivi.*

Come collaudare un firewall

Come si fa a sapere se un firewall funziona o no? Dobbiamo per forza fidarci delle dichiarazioni di affidabilità dei loro produttori? Dopotutto, ogni tanto anche i firewall rivelano qualche falla.[36] Ci vorrebbe qualcosa che mettesse alla prova il firewall con qualche tentativo di intrusione, senza però far danni. Per fortuna Internet offre numerosi servizi di questo genere.

> *Questi test funzionano correttamente soltanto se l'indirizzo IP che indicano come bersaglio quando li consultate è uguale a quello assegnato al vostro computer.*
>
> *Per conoscere il vostro indirizzo IP, scegliete* Start > Impostazioni > Connessioni di rete *e cliccate con il pulsante destro sulla connessione a Internet indicata nell'elenco che compare. Scegliete* Stato *dal menu e poi la scheda* Supporto *(Figura 5.1).*
>
> *Se gli indirizzi IP non coincidono, il test non vi dice nulla sulle difese del vostro computer, ma mette alla prova quelle del vostro fornitore d'accesso o di altri apparecchi collegati più a monte del vostro PC.*
>
> *Questo capita, per esempio, se avete più computer che condividono una connessione o siete abbonati ad alcuni fornitori ADSL o in fibra ottica. In tal caso, per collaudare il vostro firewall ci vuole un esperto che si colleghi* direttamente *al vostro computer con il suo, dotato di appositi programmi di test facilmente reperibili in Rete.*

Grc.com

Uno dei più celebri test per i firewall è disponibile presso il sito dell'esperto Steve Gibson (*grc.com*), ed è diviso in due sezioni chiamate *ShieldsUp* e *LeakTest*, alle quali si accede cliccando sui rispettivi titoli nella pagina principale del sito.

Il test della sezione ShieldsUp si attiva cliccando su *Proceed* e accettando eventuali segnalazioni di sicurezza generate da Windows o dal vostro programma di navigazione (Internet Explorer o altro).

Figura 5.1

Il sito cercherà di penetrare in modo innocuo nel vostro computer: in pratica, si comporterà come un intruso che prova tutte le maniglie di un corridoio d'albergo in cerca di qualche porta non chiusa. Se avete impostato il firewall per notificarvi dei tentativi di penetrazione, appena iniziate il test dovrebbe partire una sinfonia di allarmi.

Cliccate sui pulsanti *File Sharing* e *Common Ports* per avviare un collaudo delle "porte" che più frequentemente vengono lasciate aperte da Windows e dai più diffusi programmi.

Scegliendo *File Sharing*, se il vostro firewall funziona a dovere dovreste ottenere da Grc.com due responsi: *"Your Internet port 139 does not appear to exist"* e *"Unable to connect with NetBIOS to your computer"*.

Questi messaggi significano che il tentativo di intrusione è fallito, ossia che il firewall ha resistito correttamente. Se non ottenete questi due messaggi, siete nei guai, perché il firewall è inefficace e chiunque può entrare e leggere il contenuto del vostro computer.

Il test di *Common Ports* (Figura 5.2) è più ampio e dettagliato: esamina un maggior numero di porte e indica per ciascuna porta il risultato del tentativo di intrusione. L'ideale è ottenere un risultato *Stealth* su tutte le porte, che significa che il vostro computer risulta addirittura invisibile agli intrusi di media competenza.

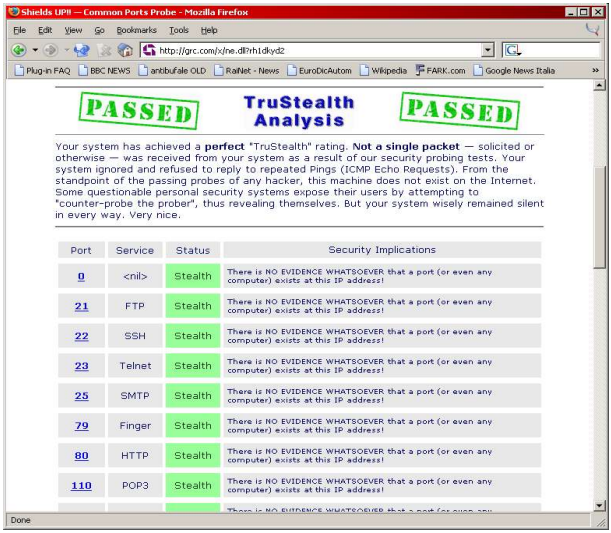

Figura 5.2

Se per varie ragioni non riuscite a ottenere questo risultato, potete comunque accontentarvi tranquillamente di un *Closed*, che indica che il vostro computer è rilevabile dall'esterno tramite quella porta ma saggiamente respinge l'intrusione. Ai fini pratici, fra *Closed* e *Stealth* non c'è poi grande differenza: l'importante è che il vostro computer non risponda alle chiamate provenienti dall'esterno.

Se trovate *Open* su una o più porte, siete nei guai: vuol dire che il vostro computer è non solo rilevabile, ma addirittura risponde ai tentativi di presa di contatto dall'esterno, che possono essere il primo passo di un'intrusione. Se non avete una ragione più che valida per lasciare aperte queste porte (per esempio ospitate un server Web o FTP e quindi dovete lasciare aperte le porte 80 o 21), è meglio che cominciate a preoccuparvi e chiedete un consulto a un esperto sul posto.

Se vi occorre un test ancora più approfondito, potete scegliere una terza opzione, *All Service ports*, che esamina un numero molto ampio di porte (le prime 1056) e le diagnostica individualmente con un semaforo verde (tutto OK, siete invisibili), blu (porta chiusa ma rilevabile) o rosso (porta aperta e vulnerabile).

In realtà neppure questo test approfondito esamina tutte le porte, che sono in realtà ben 65535 e possono essere usate ciascuna in due modi (TCP e UDP); se volete collaudare altre porte, potete scegliere l'opzione *User Specified Custom Port Probe*, specificandone fino a sessantacinque per volta.

Dopo le prime 1056 verificabili con gli altri test, le porte più a rischio, perché usate da programmi molto diffusi, e quindi le più meritevoli di un test personalizzato sono le seguenti (fra parentesi il programma o il servizio Windows che le usa):

- TCP 1503 (NetMeeting), UDP 1701 (L2TP), TCP 1720 (NetMeeting), TCP/UDP 1723 (PPTP), TCP 1731 (NetMeeting), UDP 1900 (SSDP), UDP 2001-2120 (Windows Messenger), TCP 2869 (Universal Plug and Play), TCP 3002 e 3003 (Condivisione Connessione Internet), TCP 3389 (RDP), TCP 5000 (Universal Plug and Play), UDP 6801 (Windows Messenger), TCP 6891-6900 e TCP/UDP 6901 (Windows Messenger).

Queste porte devono essere aperte se usate i servizi o programmi associati ad esse; altrimenti devono risultare chiuse.

La sezione *LeakTest* è ancora più severa: consente di collaudare la robustezza del vostro firewall per quel che riguarda i tentativi di *uscita* dal vostro computer. Per usarla, scaricate un piccolissimo quanto innocuo programma che simula il comportamento di un programma ostile, lo depositate in una cartella di prova e lo rinominate, dandogli il nome di un altro programma che avete già autorizzato (per esempio *svchost.exe*).

Se il vostro firewall è stupido e identifica i programmi autorizzati soltanto sulla base del loro nome e non del loro contenuto, il programma di prova riuscirà a uscire e contatterà *Grc.com*, avvisandovi del successo del test (e quindi del fallimento del vostro firewall). Se il vostro firewall si accorge dell'impostura, bloccherà il programma di prova, come mostrato nella Figura 5.3 nel caso di Zone Alarm.

Altri test per il vostro firewall

Alcuni produttori di antivirus e di altro software per la sicurezza informatica offrono test gratuiti simili a quelli di Steve Gibson.

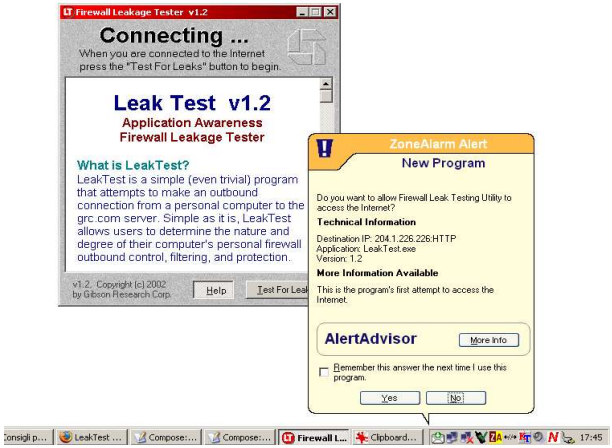

Figura 5.3

- Trend Micro, per esempio, offre *Hacker Check*, presso *www.hackercheck.com*. Il servizio è in inglese e richiede una conferma di autorizzazione preventiva via e-mail.
- Anche Sygate offre un servizio analogo, sempre in inglese, presso *scan.sygate.com*.
- Se volete qualcosa in italiano, potete usare il test di Symantec, disponibile presso questo chilometrico indirizzo:

  security.symantec.com/default.asp?productid=symhome&langid=it&venid=sym

  Secondo quanto indicato da Symantec, il test funziona soltanto con Internet Explorer e Netscape e richiede di accettare l'installazione di un piccolo programma apposito.

Problemi di dentizione

Le prime volte che si usa un firewall, capita che alcuni programmi cessino di funzionare. Il problema più classico è che diventa improvvisamente impossibile usare Internet Explorer, che prende a rispondere con il suo solito messaggio *"impossibile visualizzare la pagina"*. Usando un altro programma di navigazione, invece, la pagina Web desiderata è perfettamente visualizzabile.

La causa più frequente di questo problema è che avete detto al firewall di vietare permanentemente a Internet Explorer di uscire, invece di dirgli di chiedervi il permesso ogni volta.

Se Internet Explorer è bloccato automaticamente, non riesce a uscire dal vostro computer e quindi non può contattare il sito desiderato. Internet Explorer segnala il problema nell'unico modo che gli è dato, ossia dicendo (in tutta sincerità) che non riesce a visualizzare la pagina desiderata. Purtroppo non è abbastanza furbo da dirvi perché.

Cosa cambia con il Service Pack 2

Una delle novità di maggiore spicco del Service Pack 2 è la presenza di una versione potenziata e soprattutto attivata automaticamente del firewall già presente in XP, ribattezzata *Windows Firewall.*

È comunque consigliabile adottare un firewall alternativo, perché le prestazioni di Windows Firewall sono piuttosto limitate ed è già nota almeno una sua falla grave che in alcuni casi può rendere visibili a tutta Internet eventuali cartelle condivise del vostro PC.[37]

Per fortuna, Microsoft ha avuto il buon senso di collaborare con le società che producono firewall alternativi e quindi se installate un altro firewall, Windows Firewall si disattiva automaticamente e cede il comando al concorrente.

Come con qualsiasi firewall, ci possono essere interferenze con il funzionamento di alcuni programmi che devono scambiare dati con altri computer della rete locale o su Internet (per esempio i programmi di scambio file come WinMX, Kazaa o eMule). In tal caso occorre accedere alla schermata di configurazione di Windows Firewall (*Start* > *Impostazioni* > *Pannello di controllo* > *Windows Firewall*, oppure clic destro sull'icona di connessione nell'area di notifica) e aprire le porte usate da questi programmi.

Windows Firewall è comunque già preimpostato in modo da non interferire con il traffico generato dai programmi più diffusi e con quello generato all'interno di una rete locale, per cui le condivisioni delle stampanti e dei file non dovrebbero subire interferenze. In ogni caso, sul sito Microsoft è disponibile una miniguida di configurazione in italiano.[38]

È possibile creare una lista di *eccezioni*, ossia di programmi autorizzati a *ricevere* comunicazioni dall'esterno. Questo è utile per i giochi online e per i programmi di scambio e di chat come MSN Messenger, che devono poter ricevere istruzioni dall'esterno. Si

possono anche definire porte specifiche che il firewall deve lasciare aperte (mi raccomando, fatelo soltanto con molta cautela).

> *È altamente sconsigliabile attivare la Condivisione file e stampanti se il vostro computer è collegato direttamente a Internet. Un aggressore può far leva su questo servizio e accedere ai file condivisi.*[39]
>
> *Questo è un tranello particolarmente insidioso per chi usa il PC in ufficio e condivide file con la rete aziendale e poi usa lo stesso computer collegandosi direttamente alla Rete: è facile dimenticarsi di disattivare la condivisione, esponendosi quindi a un rischio notevole.*
>
> *Se avete bisogno di attivare la Condivisione file e stampanti, attrezzatevi con un firewall hardware che si interponga fra il vostro computer e Internet.*

Il firewall di Microsoft include anche una modalità "chiudere i boccaporti" facilmente attivabile tramite la casella *Non consentire eccezioni*. Questa modalità va usata per le situazioni a rischio (Figura 5.4): per esempio, in occasione di un attacco virale particolarmente grave e pervasivo o quando viene scoperta una vulnerabilità in un'applicazione o in un componente di Windows che accede a Internet.

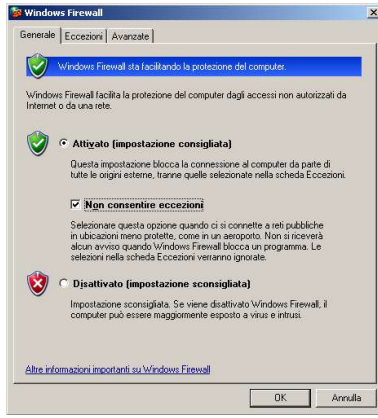

Figura 5.4

Un'altra situazione in cui è opportuno "chiudere i boccaporti" è quando si effettua una connessione a Internet al di fuori della protezione della rete aziendale (come fa tipicamente il *manager* che si porta il PC portatile dell'ufficio a casa).

In questa modalità vengono scavalcate tutte le eccezioni che avete definito e quindi viene rifiutata ogni comunicazione iniziata **dall'esterno**: sono ammesse soltanto quelle in partenza dal vostro computer, che in teoria dovrebbero essere legittime. In teoria.[40]

Libera uscita

L'integrazione di un firewall rimodernato in Windows XP non significa che si possono buttar via i firewall prodotti da terzi. Il prodotto Microsoft ha al momento, anche nella sua incarnazione nel Service Pack 2, una limitazione non presente in molti dei suoi concorrenti: **consente automaticamente tutte le connessioni *in uscita*, a prescindere dal programma che le genera**.[41]

Detta così può sembrare una cosa poco importante. Che problema c'è? Se un programma *esce* dal vostro computer, è perché volete che esca, no? Quindi non c'è ragione di mettere blocchi in uscita: l'importante è che ci siano quelli in entrata, per tenere fuori i cattivi, e il firewall Microsoft li ha.

Purtroppo non è così semplice. Mettiamo che veniate infettati da un virus informatico o da uno dei loro cugini molesti, gli *spyware* (descritti in dettaglio in seguito): i tentativi di questi programmi ostili di raggiungere il proprio padrone o di disseminarsi **non verranno fermati** da Windows Firewall, come avviene invece con i firewall alternativi. Sarete insomma non soltanto infetti, ma anche untori.

In conclusione, il firewall integrato nel Service Pack 2 è meglio del colabrodo cosmico che Microsoft offriva prima e permette di collegare un PC Windows a Internet senza che si infetti automaticamente entro pochi minuti, ma non è ancora adeguato ai problemi di sicurezza odierni. Problemi di lingua e di costi a parte, vi troverete meglio con un firewall alternativo.

Capitolo 6

Antivirus

I virus sono la minaccia più frequente, universale e dannosa per la normale impostazione di Windows. È praticamente impossibile frequentare Internet e non imbattersi in queste pestifere creature.

Anche se siamo astuti e prudenti, sicuramente fra i nostri amici, colleghi e conoscenti c'è qualcuno che si fa fregare, s'infetta e di conseguenza manda involontariamente virus a tutti quelli che conosce e quindi anche a noi.

Inoltre i virus sono furbi: i loro creatori sfruttano non solo le proprie competenze tecnologiche, ma anche la propria conoscenza dei punti deboli della psicologia umana per tentare di abbindolarci.

È per questo che la semplice prudenza non basta: ci vuole anche uno strumento freddo e razionale come può esserlo solo un programma per computer. La razionalità dell'antivirus e l'istinto umano, se messi insieme e adeguatamente addestrati, sono una combinazione potentissima. Ecco perché l'antivirus è al secondo posto nel Dodecalogo:

> ***Regola 2. Installate un buon antivirus, tenetelo costantemente aggiornato e usatelo su tutti i file che ricevete.***

Capire i virus

Per debellare il nemico bisogna conoscerlo. In termini molto generici, un *virus* è un programma ostile, che agisce nel vostro computer senza il vostro consenso e fa qualcosa che non desiderate che faccia: di solito fa danni o abusa del vostro computer o della vostra connessione a Internet. Molti obiettano sarcasticamente che anche Windows è un virus, secondo questa definizione. È un concetto da ponderare.

Un virus può causare danni di ogni sorta: per esempio, può cancellare i vostri documenti, alterarne il contenuto, paralizzarvi il computer, inviare messaggi pubblicitari a vostra insaputa, spiare il vostro lavoro al computer, addebitarvi telefonate salatissime in bol-

letta e così via. Certi virus sono capaci di accendervi il microfono e la *webcam* (la telecamerina che molti collegano al computer) e spiarvi di nascosto, ascoltando tutto quello che dite. Creature simpatiche, vero?

Come si propaga un virus

Un virus può infettare il vostro computer in tanti modi. Quello più frequente, ma non l'unico, è l'e-mail: **il virus arriva come allegato a un messaggio**.

> *C'è sempre qualcuno che a questo punto obietta* "ma a me l'antivirus non serve, tanto non apro gli allegati"*. Errore. Molti virus sono in grado di colpire Windows anche senza che apriate un allegato.*[42]
>
> *Inoltre molte versioni meno recenti ma tuttora in circolazione dei programmi di Microsoft (e di altri produttori) non solo aprono* ***automaticamente*** *gli allegati, ma eseguono altrettanto automaticamente eventuali comandi inseriti nel corpo del testo di un messaggio, per cui* ***anche i messaggi senza allegato sono pericolosi, se usate questi programmi.***
>
> *Alcuni virus, se colpiscono computer con Internet Explorer e/o Outlook Express non aggiornati, riescono a farsi eseguire semplicemente* ***visualizzando l'anteprima*** *del messaggio al quale sono allegati.*

Ricordatevi di **non fidarvi del mittente di un messaggio contenente allegati**, chiunque sia o sembri essere, specialmente se sembra essere un mittente apparentemente autorevole, un amico o un collega (Regola 8). I virus falsificano quasi sempre il mittente proprio per indurvi a concedere loro fiducia.

L'e-mail è il vettore d'infezione principale, ma ne esistono molti altri. Per esempio:

- **le pagine Web:** in determinate circostanze, purtroppo piuttosto comuni, è sufficiente visualizzare una pagina Web per infettare il proprio computer.[43]
- **file di documenti, programmi, video, musica:** il virus può insediarsi in pratica in **qualsiasi file** che scarichiamo da Internet

o che troviamo in un CD, DVD o un dischetto. Eseguendo il programma, aprendo il documento o semplicemente inserendo il disco, il virus si propaga al nostro computer. Per esempio, i documenti Word sono uno dei veicoli di infezione più sfruttati, grazie ai cosiddetti *macrovirus*.
Persino i videoclip sono vettori di virus, perché possono includere comandi che scaricano ed eseguono automaticamente il virus vero e proprio dal sito dell'aggressore.

- **programmi o file scaricati dai circuiti di scambio tipo eMule, Kazaa o WinMX:** il materiale che trovate in questi circuiti è distribuito senza garanzia e spesso nell'illegalità. Le copie pirata di programmi commerciali sono spesso infettate intenzionalmente dagli aggressori perché costituiscono un'ottima esca.
- **messaggi istantanei:** quelli di programmi per “chattare” come *Messenger* e come quelli che usano il sistema IRC, specialmente se trasportano file.
- **dischetti, anche vuoti:** alcuni virus, i *boot virus*, sono in grado di infettare un dischetto e "nascondersi" in modo che il dischetto sembri vuoto. Se avviate il computer tenendo inserito quel dischetto e non avete preso precauzioni, il virus si autoinstalla e contamina il vostro PC, scavalcando astutamente l'antivirus perché normalmente il computer esegue il contenuto del dischetto (infetto) ancor prima di avviare Windows e l'antivirus.
  Anche un CD/DVD di dubbia provenienza (software pirata, per esempio) può contenere virus basati sullo stesso principio.
- **la rete locale di computer:** i cosiddetti *worm* si propagano automaticamente da un computer all'altro della medesima rete locale, attaccando persino le stampanti di rete, e infettano senza ricorrere a e-mail, file o allegati.
  Di conseguenza, se un computer non è ben protetto, può ricevere l'infezione dagli altri computer presenti nell'ufficio o nell'ambiente di lavoro. Non fidatevi di nessuno!

> *Un virus può infettare **praticamente qualsiasi file** e **può propagarsi via e-mail senza usare il vostro programma di posta**.*
>
> *Molti virus leggono la rubrica di indirizzi della vittima e la usano per trovare nuovi bersagli. Così le nuove vittime ricevono un allegato da una persona che conoscono e*

*quindi se ne fidano e si infettano. È per questo che **non bisogna fidarsi dei messaggi che sembrano provenire da conoscenti**.*

*Inoltre, quasi tutti i virus **falsificano il mittente** in vari modi per nascondere le proprie tracce.*

Chi crea i virus?

Sono quasi finiti i tempi in cui il creatore di virus era un ragazzino in crisi ormonale che sfogava la mancanza di morosa con un gesto vandalico. Ogni tanto qualcuno di questi sfigati riemerge dalla sua cameretta e compie devastazioni per vantarsi con gli amici altrettanto sfigati della sua cerchia, ma oggi il fenomeno virus è prevalentemente **commerciale**.

Molti dei virus più diffusi, infatti, non producono danni diretti alle vittime: le **infettano con discrezione** per usarle come insospettabili teste di ponte, dalle quali lanciare attacchi informatici a siti importanti (come Google o Microsoft) o bombardamenti pubblicitari (il cosiddetto *spam*) verso altri utenti, intasando le caselle di posta di mezzo mondo con improbabili réclame di prodotti per allungare, rassodare, sollevare e ingrandire ogni parte del corpo maschile e femminile.

Un attacco virale ben congegnato infetta segretamente milioni di computer, creando una vera e propria "rete nella Rete" che ubbidisce ai comandi del misterioso untore. Il danno nasce quando questi bombardamenti si fanno così intensi da paralizzare il traffico verso il sito bersagliato o soffocare in una marea di messaggi inutili gli e-mail che ci interessano.

Spesso l'utente infetto non si accorge di essere la fonte di questi attacchi e/o e-mail pubblicitari, ma se ne accorgono i servizi di sorveglianza di Internet, che gli "tagliano la linea" vietandogli di inviare qualsiasi messaggio, compresi quelli legittimi, con i danni e disagi che questo comporta.

In sostanza, è come se un televenditore senza scrupoli si allacciasse di nascosto al vostro telefono per chiamare migliaia di persone, molestandole con il suo messaggio pubblicitario. A un certo punto i molestati segnalerebbero il problema e l'operatore telefoni-

co risalirebbe alla fonte, cioè voi, staccandovi la linea per impedirvi ulteriori molestie.

> *C'è una diceria molto diffusa secondo la quale i virus verrebbero creati dai produttori di antivirus per crearsi un mercato. È un po' come sospettare che i vetrai assoldino i ragazzini con le fionde per rompere le finestre, o che i fabbricanti di casseforti finanzino gli scassinatori.*
>
> *Ne ho parlato con alcuni rappresentanti di società produttrici di antivirus, che mi hanno risposto molto divertiti: per loro fortuna, mi dicono, non hanno bisogno di pagare nessuno per creare virus, perché ci pensano già gratuitamente, e fin troppo abbondantemente, i vandali della Rete. Scriverne altri sarebbe un costo aggiuntivo inutile.*

Insomma, i danni causati da un'infezione informatica sono serissimi. Sbarazzarsene è difficile: disinfestare un computer infetto è un'operazione delicata. Per questo **è fondamentale la prevenzione**. Una volta che siete infetti, spesso è troppo tardi.

Come funziona un antivirus

Un antivirus è un programma che sorveglia l'attività del vostro computer e riconosce i tipici segni di comportamento sospetto. Solitamente gli antivirus attingono a uno "schedario" di "foto segnaletiche" di virus conosciuti.

Quando ricevete un allegato o chiedete all'antivirus di verificare un file scaricato da Internet o presente su un disco, l'antivirus confronta il contenuto del file (o il traffico di dati da e verso Internet) con il contenuto del proprio schedario: se trova una corrispondenza, segnala la presenza di un virus; se non la trova, dichiara che il file è "pulito".

> *Se vi interessano i dettagli tecnici, queste "foto segnaletiche" sono costituite da brevi sequenze di byte notoriamente presenti nei vari virus. Se una di queste sequenze viene rilevata in un file, l'antivirus ritiene che il file sia infetto.*

Questo modo di operare contribuisce molto alla prevenzione, ma non è perfetto. Infatti **l'antivirus può riconoscere soltanto i virus già catalogati nel suo schedario.** È come se un poliziotto fosse in grado di riconoscere e arrestare soltanto i pregiudicati.

Ogni volta che esce un nuovo virus, evento peraltro frequentissimo, i produttori di antivirus aggiornano lo schedario con la "foto segnaletica" del nuovo pericolo. Ma **finché non forniamo al nostro antivirus lo schedario aggiornato, l'antivirus non riconoscerà la nuova minaccia**.

È per questo che **l'antivirus richiede aggiornamenti continui**. Usare un antivirus senza aggiornarlo, come purtroppo fanno in tanti, è peggio che non usarlo del tutto: si crede di essere protetti quando non lo si è e quindi si abbassa la guardia.

Tuttavia, difendersi dai virus non significa semplicemente usare un antivirus e non pensarci più: richiede anche un **comportamento prudente**, descritto nelle altre regole del Dodecalogo e nelle prossime pagine.

Installare un buon antivirus

Una delle ragioni per cui le invasioni di virus continuano a esistere nonostante ci siano gli antivirus è che molti utenti sono riluttanti a usare un antivirus. Credono che rallenti il computer e debba essere costoso. Forse non si rendono conto quanto costi un'infezione in termini di tempo e dati persi: è una di quelle lezioni che si imparano soltanto vivendole di persona.

In realtà i costi sono un falso problema: infatti accanto ai programmi commerciali a pagamento, nei quali spesso tocca pagare sia il programma, sia i frequenti aggiornamenti del suo "schedario", ci sono **ottimi antivirus gratuiti**.

La differenza fra i programmi gratuiti e quelli a pagamento è principalmente una questione di lingua (talvolta quelli gratuiti non sono in italiano) e di celerità nell'aggiornare lo "schedario". Gli antivirus gratuiti tendono inoltre a essere più leggeri ed essenziali rispetto a quelli commerciali, spesso afflitti dalla Sindrome della Tazzina (nel senso di *"faccio tutto, anche il caffè"*), risolvendo così la preoccupazione di rallentare il PC.

Entrambi sono comunque validi strumenti di difesa, sia pure con le limitazioni descritte nella seconda parte di questo capitolo.

> ***Non installate più di un antivirus.*** *Potreste pensare che due antivirus sono meglio di uno e che uno possa supplire a eventuali carenze dell'altro. Purtroppo, come i proverbiali due galli nel pollaio, gli antivirus di norma tollerano poco la compresenza di "colleghi" e in ogni caso il rischio di creare complicazioni inutili è alto.*

Antivirus a scelta

C'è soltanto l'imbarazzo della scelta, fra versioni italiane e in lingua straniera, gratuite e a pagamento, "rustiche" o superaccessoriate. Ecco un breve elenco di alcuni degli antivirus più gettonati.

- **Nome:** Antivir Personal Edition
  Produttore e sito: H+BEDV Datentechnik GmbH, www.free-av.com
  Prezzo: gratuito per uso personale
  Lingua: inglese o tedesco
- **Nome:** Antiviral ToolKit Pro (AVP), Kaspersky Antivirus
  Produttore e sito: Kaspersky, www.kaspersky.it
  Prezzo: a pagamento, disponibile versione di valutazione gratuita scaricabile
  Lingua: italiano
- **Nome:** Avast Home Edition
  Produttore e sito: Alwil Software, www.avast.it
  Prezzo: gratuito
  Lingua: italiano
- **Nome:** AVG Free
  Produttore e sito: Grisoft, www.grisoft.com
  Prezzo: gratuito per uso personale
  Lingua: inglese
- **Nome:** BitDefender
  Produttore e sito: Softwin, it.bitdefender.com
  Prezzo: a pagamento, disponibile versione di valutazione gratuita scaricabile e versione per DOS utilizzabile anche per disinfezione di Windows
  Lingua: italiano
- **Nome:** ClamWin
  Produttore e sito: la comunità degli informatici, www.clamwin.com

Prezzo: gratuito
Lingua: inglese, ma essendo software libero chiunque può tradurlo

- **Nome:** eTrust EZ Antivirus Protection
  Produttore e sito: Computer Associates, www.my-etrust.com/products/Antivirus.cfm
  Prezzo: a pagamento
  Lingua: inglese
- **Nome:** F-Prot
  Produttore e sito: Frisk Software International, www.f-prot.com
  Prezzo: a pagamento, disponibile versione di valutazione gratuita scaricabile e versione per DOS utilizzabile anche per disinfezione di Windows
  Lingua: inglese
- **Nome:** F-secure
  Produttore e sito: F-Secure, www.f-secure.it
  Prezzo: a pagamento; disponibile versione di valutazione gratuita scaricabile
  Lingua: italiano
- **Nome:** McAfee VirusScan
  Produttore e sito: McAfee, it.mcafee.com
  Prezzo: a pagamento
  Lingua: italiano
- **Nome:** Nod32
  Produttore e sito: distribuito in Italia da Future Time Srl, www.nod32.it
  Prezzo: a pagamento (in prova per 30 giorni), pagabile anche con conto corrente postale
  Lingua: italiano
- **Nome:** Norton Antivirus
  Produttore e sito: Symantec, www.symantec.it/region/it/product/nav_index.html
  Prezzo: a pagamento
  Lingua: italiano
- **Nome:** PC-Cillin
  Produttore e sito: Trend Micro, it.trendmicro-europe.com
  Prezzo: a pagamento, disponibile versione di valutazione gratuita scaricabile
  Lingua: italiano
- **Nome:** Sophos Anti-Virus
  Produttore e sito: Sophos, www.sophos.it

Prezzo: a pagamento, disponibile versione di valutazione gratuita scaricabile

Lingua: italiano

Sul mio sito www.attivissimo.net*, nella sezione dedicata a questo libro, trovate le istruzioni dettagliate per scaricare, installare e configurare AVG, l'antivirus che uso sui miei computer Windows.*

Anche se scegliete di non usare questo antivirus, leggetele comunque: i principi presentati sono validi per quasi tutti i programmi analoghi.

Non fidatevi delle vecchie edizioni di antivirus talvolta disponibili a prezzo scontato nei negozi: spesso sono incompatibili con Windows XP e non rilevano correttamente i virus anche se scaricate i loro aggiornamenti. Acquistate sempre la versione più recente del prodotto.[44]

L'antivirus che non si installa

Tutti gli antivirus presentati nella tabella precedente sono programmi abbastanza tradizionali, fatti per essere scaricati (o acquistati in negozio) e installati.

Tuttavia ci sono altri antivirus che fanno sostanzialmente a meno dell'installazione tradizionale, perché vengono eseguiti direttamente via Internet: non si fa altro che visitare il relativo sito Web e cliccare sul pulsante di inizio verifica. Nel vostro computer viene installato soltanto un piccolo componente dell'antivirus, che non è un programma autonomo ma si appoggia al programma *browser* che usate per la navigazione (di solito Internet Explorer).[45]

Questa soluzione è utile nel caso di un computer già infetto con uno dei tanti virus che disattivano gli antivirus convenzionali, oppure per un rapido controllo preliminare di un computer non ancora dotato di antivirus.

Non va considerato, comunque, come un sostituto completo di un antivirus "tradizionale", perché quasi sempre ha bisogno di restare collegato a Internet, dipende dall'uso di Internet Explorer e non è

veloce quanto un antivirus installato; cosa più importante, non permette di intercettare al volo eventuali file infetti che ricevete nella posta o da un sito Web (l'antivirus tradizionale sì).

Ecco alcuni esempi di dove reperire questi antivirus "senza installazione":

- **F-Secure:** *support.f-secure.com/enu/home/ols.shtml*
- **Trend Micro:**
  it.trendmicro-europe.com/consumer/products/housecall_pre.php
- **Panda antivirus:**
  www.pandasoftware.com/activescan/it/activescan_principal.htm
- **Symantec:**
  security.symantec.com/sscv6/home.asp?langid=it&venid=sym&close_parent=true

Quasi tutti i produttori citati nell'elenco precedente di antivirus da installare, inoltre, offrono anche questo tipo di prodotto senza installazione.

L'antivirus su misura

Un'altra soluzione di emergenza per ripulire un computer infetto è costituita dagli antivirus su misura, detti anche *cleaner*, offerti gratuitamente da molte società che producono antivirus. Si tratta di piccolissimi programmi concepiti per eliminare uno o più tipi specifici di virus. Un esempio di questi *cleaner* è *Stinger*, di McAfee (*vil.nai.com/vil/stinger*).

I *cleaner* hanno effetto soltanto sui tipi di virus per il quale sono progettati, ma rispetto agli antivirus generici hanno il vantaggio di essere sempre gratuiti, di essere facilmente scaricabili e trasportabili su dischetto e di non richiedere un'installazione complicata.

Chiaramente un antivirus su misura presuppone che l'utente sappia già quale virus l'ha infettato. In genere non è difficile scoprirlo: quasi tutti i virus producono effetti abbastanza caratteristici nel computer infetto (messaggi a video, alterazioni dei file principali di Windows, spegnimento improvviso del computer e via dicendo).

Inoltre capita a volte che un antivirus "normale" riconosca il virus ma non riesca a debellarlo. In questo caso i *cleaner* diventano

spesso l'unico modo per liberarsi agevolmente dei virus che sono abbastanza astuti da resistere ai normali antivirus generici.

Non fidatevi degli e-mail che sembrano provenire da società affidabili e vi offrono un "antivirus su misura" allegato al messaggio: *sono tentativi di infettarvi. Il mittente è falso e l'allegato è in realtà un virus.*

Configurare l'antivirus

La configurazione di un antivirus è semplice, ma va fatta con attenzione, in modo da non lasciare "zone morte" nel computer dove il virus possa acquattarsi per poi riemergere e reinfettare (ebbene sì, si chiamano "virus" proprio perché imitano il comportamento dei loro omonimi biologici).

- **File grandi e piccini.** Molti antivirus sono impostati in modo da non esaminare i file oltre una certa dimensione. La teoria è che i virus raramente infettano file molto grandi come gli archivi di dati o i video, per cui si risparmia tempo se non li si esamina.
  In pratica, però, gli autori di virus non sono stupidi e sanno come funzionano gli antivirus, per cui tendono sempre più spesso a nascondere copie dei loro virus proprio in questi file normalmente non esaminati.
  Pertanto è importante impostare l'antivirus in modo che esamini *qualsiasi* file, a prescindere dalle sue dimensioni. L'esame richiederà più tempo, ma è un male necessario.
- **Tutti i tipi di file.** Capita spesso che un antivirus si limiti, se non si interviene manualmente, a esaminare soltanto i tipi di file che ritiene siano "a rischio": tipicamente i file eseguibili (con estensioni come *exe, com, bat, pif*, *scr* e altre).
  Come nel caso precedente, anche qui il rischio è che emerga un virus che si camuffa attaccandosi a file aventi estensioni ritenute fino a quel momento "sicure" e quindi sfugga al controllo dell'antivirus.
  Oltretutto abbiamo visto che la vera estensione di un file è facilmente mascherabile in Windows. Meglio quindi impostare l'antivirus in modo che esamini ogni e qualsiasi file, a prescindere dal tipo.
- **Scansione dell'e-mail.** Buona parte degli antivirus è in grado di esaminare in tempo reale gli allegati ricevuti nella posta e

bloccare quelli pericolosi.
Questa funzione è preziosissima nella posta in *entrata*, ma talvolta causa problemi quando è attivata per la posta in *uscita*, perché i messaggi filtrati che produce vengono interpretati da alcuni programmi di posta come se fossero accompagnati da un allegato (in realtà inesistente), suscitando confusione e allarme inutile in chi li riceve.
Se ricevete lamentele a proposito di allegati fantasma dai vostri conoscenti, vi conviene quindi disattivare il controllo antivirus dei messaggi uscenti (anche perché si presume che se siete stati attenti, non siete infetti, quindi non potete inviare e-mail infetti, vero?).

- **Aggiornamenti automatici o manuali?** Di solito si può scegliere fra scaricare automaticamente gli aggiornamenti a un'ora e un giorno della settimana prestabiliti oppure provvedere manualmente.
  Il vantaggio dell'automatismo è che vi toglie l'incombenza di ricordarvi di aggiornare l'antivirus; il suo svantaggio è che comporta che sia costantemente in esecuzione (e venga caricata ogni volta all'avvio del computer) la parte dell'antivirus dedicata a guardare che ore sono e che giorno è per decidere se è il momento di scaricare o no.
  Questo può rallentare l'avvio e il funzionamento di Windows, e se non siete permanentemente connessi a Internet può infastidire con i suoi tentativi automatici di connettersi. Se siete tipi metodici e parsimoniosi, vi conviene disattivare l'automatismo.
- **Monitoraggio continuo o no?** Quasi tutti gli antivirus restano permanentemente in esecuzione e sorvegliano tutti i file che ricevete, controllandoli in tempo reale.
  Questo è molto utile, ma comporta un aggravio di utilizzo della memoria di lavoro (RAM) del computer e rallenta in generale l'accesso al disco rigido.
  Se non vi occorre un monitoraggio continuo, per esempio perché avete un computer portatile che collegate saltuariamente a Internet e nel quale non immettete file provenienti da altre fonti, potete anche disattivarlo e alleggerire il carico di lavoro del PC.
  Se non avete problemi di risorse del computer, però, lasciate attivo questo monitoraggio: è più prudente.
- **Che fare dei virus scovati?** Non lasciatevi tentare dalla curiosità, cattiva consigliera: non aprite mai un virus *"tanto per ve-*

dere cosa c'è dentro".
Alcuni antivirus consentono di "mettere in quarantena" i file ritenuti infetti o i virus identificati con certezza. Personalmente trovo sia una possibilità troppo pericolosa. Conservare i virus non serve a nulla, se non agli esperti di settore per eventuali indagini, e può comportare un'infezione dovuta a un errore di manovra. Terreste in casa un flacone di vaiolo? Appunto.
Isolare un file infetto può sembrare un'opzione utile se si tratta dell'unica copia di un file prezioso, per tentare di recuperarla, ma il recupero è talmente rischioso (e le possibilità di successo sono talmente basse) che raramente ne vale la pena.
Conviene insomma dire all'antivirus di cancellare tutto ciò che trova infetto e organizzarsi preventivamente con le copie di sicurezza, come descritto nel capitolo *Backup*, in modo da non trovarsi mai con un'unica copia dei file che ci servono.

- **Notifiche.** Alcuni antivirus consentono di inviare automaticamente un e-mail di notifica a chi ci manda e-mail infetti, per avvisarlo che è infetto e sta inconsapevolmente disseminando virus a destra e a manca.
  Nobile proposito; peccato che praticamente tutti i virus attuali falsifichino il mittente, per cui l'antivirus manda la notifica a chi non c'entra nulla, causando soltanto ulteriore traffico, panico e confusione. Disattivate questa funzione, se l'avete.

Tenere costantemente aggiornato l'antivirus

A costo di ripetermi: per l'amor del cielo, **ricordatevi di tenere aggiornato il vostro antivirus.** Questo è l'errore in cui inciampano tutti i principianti. Escono virus nuovi letteralmente tutti i giorni e l'antivirus li può riconoscere soltanto se lo aggiornate. Avere un antivirus non aggiornato è un scelta di pigrizia irresponsabile quanto riciclare i preservativi usati.

L'aggiornamento può avvenire automaticamente o meno, a seconda delle impostazioni scelte e dei servizi abilitati in Windows.[46] Consiste in un breve collegamento a Internet, durante il quale l'antivirus scarica dal sito del produttore un file contenente le nuove "schede segnaletiche" dei virus comparsi di recente. L'antivirus carica gli aggiornamenti, riavviandosi se necessario, ed è pronto a riconoscere le nuove minacce.[47]

> ***Non scaricate aggiornamenti da fonti diverse dal sito del produttore dell'antivirus.*** *Un altro dei trucchi più classici degli autori di virus è confezionare un e-mail che sembra provenire da un produttore di antivirus e dice di offrire un aggiornamento gratuito, fornito nel file allegato al messaggio. L'allegato è invece un virus.*
>
> *Alcuni siti non legati ai produttori di antivirus offrono aggiornamenti scaricabili; sono da prendere con estrema cautela, perché facilmente si tratta di trappole. L'unica altra fonte di aggiornamenti di cui potete fidarvi è il CD/DVD di programmi fornito insieme ad alcune riviste d'informatica, che talvolta contiene aggiornamenti per i più diffusi antivirus.*

Cosa vuol dire "costantemente"?

L'ideale sarebbe aggiornare l'antivirus ogni volta che vi accingete ad aprire un file appena arrivato sul vostro computer, ma è una soluzione poco pratica: finirebbe per essere un impegno così oneroso che nessuno lo rispetterebbe.

Il mio consiglio è aggiornarlo **almeno una volta la settimana; meglio ancora, una volta al giorno**. Ricordate che a prescindere dalla sua cadenza, l'aggiornamento è un **obbligo**, non un consiglio, altrimenti l'antivirus non serve assolutamente a nulla.

Quando aggiornare?

Non tutti i momenti sono uguali per scaricare gli aggiornamenti. In alcuni orari, i siti dei produttori di antivirus con milioni di clienti si trovano a dover gestire un traffico enorme di utenti ansiosi di prelevare l'ultimo aggiornamento antivirus. Quando è in corso un attacco virale su vasta scala, poi, si arriva al panico generale e i siti dei produttori si intasano facilmente.

Molte aziende hanno l'abitudine di scaricare gli aggiornamenti ogni lunedì, all'inizio dell'attività lavorativa, oppure ogni mattina. Di conseguenza vi conviene evitare questi momenti per tentare di scaricare gli aggiornamenti; evitate anche i momenti in cui è mattina negli Stati Uniti (il primo pomeriggio in Italia), perché quando i milioni di utenti statunitensi si affacciano simultaneamente a Internet tutto rallenta.

Usare l'antivirus su *tutti* i file ricevuti

È facile pensare che l'unica minaccia sia costituita dai file che riceviamo da Internet, perché praticamente tutti i virus che ci perseguitano arrivano nella posta. Purtroppo non è così, e ci vuole una certa ginnastica mentale per ricordarsi di **sorvegliare tutti i canali di ingresso del computer.**

Come già descritto, un virus infatti può entrare nel computer in mille modi, molti dei quali non siamo abituati a considerare come "canali di ingresso": gli allegati all'e-mail, i programmi, la musica, i video e i documenti scaricati da siti Internet o da circuiti di scambio oppure da CD degli amici o dai circuiti di *chat*, per esempio.

Ogni volta che fate qualcosa con il vostro computer, prendete l'abitudine di chiedervi *"sta entrando qualcosa di nuovo nel mio PC? E quel "qualcosa" è stato controllato con l'antivirus aggiornato?"*.

A proposito: per brevità, quando parlo di file "ricevuti" qui e altrove, intendo sia quelli provenienti da Internet tramite la posta, sia quelli provenienti da tutti gli altri canali elencati sopra. In estrema sintesi:

> ***Tutti i file sono a rischio. Tutti i canali sono a rischio. Mai fidarsi degli amici fidati!***

Lo so, essere paranoici non è divertente, ma aiuta davvero a non farsi fregare.

Pulizie di primavera

È chiaro che è abbastanza futile sorvegliare gli ingressi del vostro computer se il nemico è già dentro. Oltre a verificare ogni file ricevuto dall'esterno, dovete quindi assicurarvi che il vostro computer non sia già infetto.

Infetto io? Non fate quella faccia. Sapeste quante volte mi è capitato di disinfestare i computer di amici e colleghi tutt'altro che sprovveduti ma totalmente ignari di essere infetti. I creatori di virus sono furbi e subdoli e cercano metodi sempre nuovi per invadere i computer. E quando c'è di mezzo una vulnerabilità intrinseca di Windows, non c'è molto che si possa fare per evitare l'infezione (anche se questo libro aiuta a contenere notevolmente il rischio).

Di conseguenza, è davvero necessario assicurarsi che nessuno dei file già presenti nel vostro computer sia infetto. Qualsiasi antivirus degno di questo nome ha una funzione apposita di *scansione completa* del computer. Occorre adoperarla subito dopo aver installato l'antivirus e **almeno una volta la settimana, subito dopo aver aggiornato l'antivirus**.

> *Alcuni virus particolarmente pestiferi sono in grado di disattivare gli antivirus convenzionali, come un ladro disattiva un antifurto per poter "lavorare" indisturbato. L'effetto è lo stesso: crediamo di essere protetti ma in realtà non lo siamo.*
>
> *Conviene pertanto usare periodicamente anche un antivirus che non richiede installazione ma agisce direttamente via Internet, come descritto nelle pagine precedenti. Questi programmi, infatti, difficilmente sono bloccabili dai virus.*
>
> *Se tutta questa manfrina vi sembra assurdamente complicata e frustrante, valutate l'ipotesi di passare a un Mac o a Linux: non avrete più problemi significativi di virus. I virus per queste alternative esistono, ma sono curiosità da laboratorio, nulla di paragonabile alle pestilenze ricorrenti che affliggono Windows.*

Limiti degli antivirus

L'antivirus è un ottimo strumento, ma non è la cura di tutti i mali. La buona sicurezza informatica, come qualsiasi altra forma di sicurezza, non si basa mai su una singola soluzione, ma su una serie di barriere, fatte in modo che se ne cede una, restano da superare le altre. Limitarsi all'antivirus è fare cattiva sicurezza informatica.

È facile pensare che un antivirus sia come un oracolo, e che se dice che un file è pulito, è sicuramente pulito, mentre se dice che è infetto, è davvero infetto. Non è proprio così. In realtà è più corretto e prudente dire che:

- se un antivirus aggiornato dice che un file è infetto, è **assai probabile (ma non certo)** che lo sia;
- se lo stesso antivirus dice che un file non è infetto, è soltanto **probabile (ma non certo)** che non lo sia.

In altre parole, anche se siete rigorosi nell'aggiornare l'antivirus, **non dovete considerarlo come una garanzia totale.** Ci sono infatti molti modi per far credere a un antivirus che un file sia "pulito" anche quando non lo è: ogni tanto qualche antivirus ritiene erroneamente infetto un file in realtà pulitissimo.

Come ti frego l'antivirus

Per esempio, gli antivirus a volte non riconoscono i cosiddetti *"dialer"*, ossia i programmi che cambiano il numero di telefono usato per collegarci a Internet e lo rimpiazzano con un costosissimo numero a pagamento tipo 899. Trovate un approfondimento nel capitolo intitolato, guarda un po', *Dialer.*

Un altro espediente usatissimo dai virus è la *compressione cifrata*. In pratica, il virus arriva come allegato sotto forma di file in formato *ZIP* (un formato molto diffuso per ridurre lo spazio occupato dai file), cifrato con un codice di protezione (*password*).

L'e-mail che accompagna il virus si spaccia per un messaggio proveniente da Microsoft, da una società di sicurezza o dal vostro fornitore d'accesso e dice che per non avere problemi dovete "decomprimere" l'allegato (in genere è sufficiente farvi sopra un doppio clic) usando il codice di protezione fornito nel messaggio ed eseguirlo. Siccome l'allegato è cifrato, l'antivirus non può aprirlo

e controllarlo, per cui solitamente lo considera erroneamente "pulito". Astuto, vero?

Un altro modo per eludere il controllo antivirus è l'uso di appositi programmi, facilmente reperibili su Internet, che consentono di creare senza fatica dei *Trojan horse*, o "cavalli di Troia", scritti su misura: programmi apparentemente innocui che racchiudono virus.

Quando la vittima lancia il programma-cavallo di Troia, sul suo computer viene eseguito il programma innocuo, per cui ha l'impressione che tutto sia a posto, ma di nascosto viene eseguito *anche il virus*.

È difficile per un antivirus riconoscere questi virus nascosti, specialmente se eseguono operazioni che potrebbero essere legittime e richieste dall'utente, come cancellare o rinominare un file oppure cambiare una parola in un documento.

Quarantena

Un'altra limitazione degli antivirus attuali è la cosiddetta *"finestra di vulnerabilità"*. Passa un certo tempo (qualche ora o più) fra l'inizio della circolazione di un nuovo virus e la disponibilità dell'aggiornamento dell'antivirus che lo riconosce. È quindi facile che un antivirus, benché fresco di aggiornamento, non riconosca un file infettato da un virus uscito poche ore prima.

Di conseguenza, la soluzione ottimale dal punto di vista della sicurezza sarebbe "mettere in quarantena" i file ricevuti (soprattutto quelli ricevuti via e-mail), ossia lasciar passare qualche ora prima di aprirli, anche se l'antivirus li dichiara puliti, poi aggiornare l'antivirus e ricontrollarli.

In questo modo, se un file ricevuto è infetto con un nuovo virus, in quel lasso di tempo verrà reso disponibile l'aggiornamento dell'antivirus che lo riconoscerà.

Purtroppo questo approccio è assurdamente scomodo. Lo scopo dell'invio di allegati via e-mail è proprio l'immediatezza della trasmissione. Per esempio, se qualcuno ci manda un allegato per lavoro, probabilmente ha bisogno che lo apriamo *subito*, non fra qualche ora.

Tutte queste tecniche di elusione possono farvi venire il sospetto che l'antivirus serva a poco e quindi non valga la pena di usarlo. Non lasciatevi tentare dalla pigrizia: la buona sicurezza è il risultato di tante barriere diverse che lavorano insieme, in modo che una compensi le lacune dell'altra.

L'antivirus riconosce ed elimina comunque *la maggioranza dei file infetti che ricevete, per cui vi risparmia molta fatica. Quelli restanti verranno riconosciuti dall'arma più potente contro gli aggressori: il vostro cervello.*

Euristi...*cosa*?

Alcuni antivirus offrono una cosiddetta *"ricerca euristica"*. Invece di basarsi esclusivamente sulle "impronte digitali" dei virus già conosciuti, la ricerca euristica si basa sul *comportamento* di un file eseguibile, in modo da poter bloccare anche virus non ancora noti.

Se un file sconosciuto si comporta in maniera sospetta (per esempio cerca di modificare parti vitali di Windows, di formattare un disco o di cancellare dati, oppure contiene istruzioni in tal senso), l'antivirus euristico lo segnala come virus.

Sulla carta sembra una bella idea: in pratica, purtroppo, la ricerca euristica tende a considerare virus anche programmi innocui che per ragioni validissime manifestano quei comportamenti sospetti (per esempio, programmi di amministrazione del disco come Partition Magic), per cui l'antivirus euristico grida spesso erroneamente *"al lupo, al lupo"*.

Il mio consiglio è lasciare disattivata la ricerca euristica per evitare falsi allarmi. Piuttosto che fidarsi dell'intelligenza del computer, conviene affinare la propria.

Cervello al contrattacco

Affidarsi totalmente all'antivirus è insomma imprudente. In casi come questi occorre far uso del migliore strumento di sicurezza oggi esistente: la materia grigia che sta appollaiata fra le vostre orecchie. Addestrata adeguatamente, riconosce praticamente tutti gli espedienti virali.

Quando si riceve un e-mail con un allegato occorre seguire una procedura semplice ma necessaria:

- **Non aprite mai un allegato usando l'apposita funzione del programma di posta:** è facilmente ingannabile. Salvate invece l'allegato su disco.
- **Controllate l'allegato con l'antivirus appena aggiornato** (questo controllo avviene quasi sempre automaticamente).
- Grazie alle modifiche che avete apportato a Windows nei capitoli precedenti, **esaminate il nome del file allegato** per capire qual è la sua *vera* estensione e se si tratta di un'estensione pericolosa o meno; i messaggi con estensioni probabilmente non pericolose (*txt*, per esempio) possono essere aperti subito, a patto che siate sicuri che quella sia la loro vera estensione e che usiate comunque il metodo "apri con" descritto nel Capitolo 3.
- **Guardate qual è la fonte apparente** del messaggio, tenendo presente che il mittente di un e-mail è facilmente falsificabile e che **nessuna società di software, specialmente Microsoft, manda allegati da installare** (al massimo manda *documenti* non installabili; di certo non manda programmi). Se la fonte non vi è familiare, conviene cestinare senza aprire l'allegato, perché episodi come questo sono così frequenti che Microsoft ha addirittura una pagina apposita di smentita.[48] [49]
- Chiunque sia o sembri essere il mittente, **non installate mai nessun programma** che ricevete come allegato.
- **Esaminate il testo del messaggio** per vedere se è per caso un testo standard confezionato da qualche autore di virus; per esempio, ci sono virus che falsificano il mittente e si spacciano per il vostro fornitore d'accesso o un'altra fonte autorevole, esortandovi ad installare il file allegato "per ragioni di sicurezza", ma si tradiscono perché ci scrivono in inglese o usano frasi generiche.
- **Se il mittente è qualcuno che conoscete, contattatelo** (anche telefonicamente, se necessario) per verificare che sia davvero lui o lei il mittente e che abbia davvero voluto inviarvi un allegato, facendo particolare attenzione ai messaggi che dicono semplicemente *"Guarda che belle foto!"* oppure *"Ecco il file che mi hai chiesto"* o usano altri testi vaghi e poco circostanzia-

ti (chi vi conosce userà di solito frasi più personalizzate e specifiche).

- Chiedetevi comunque se **è davvero necessario aprire subito** l'allegato o se potete attendere qualche ora di quarantena.

Traditi dal mezzo meccanico

Affinché antivirus e cervello possano lavorare insieme efficacemente, è importantissimo che non possano essere traditi dagli strumenti informatici sottostanti.

Per esempio, è inutile mettere in atto tutte queste difese se poi usate un programma di posta che apre automaticamente tutto quello che riceve, scavalcando l'antivirus e il buon senso. È altrettanto inutile darsi da fare con l'antivirus se il programma che usate per navigare in Internet (il *browser*) esegue qualsiasi programma annidato in una pagina Web.

Per questo **l'antivirus è soltanto il primo passo** e **occorre usare programmi sicuri per la posta e per Internet**, come descritto nelle altre regole del Dodecalogo.

La via crucis della difesa dai virus non è ancora finita. Ora sapete perché gli utenti Mac e Linux hanno spesso quell'aria compiaciuta.

Come collaudare un antivirus

Di solito non ci vuole molto per collaudare un antivirus: basta scaricare un po' di posta per trovarsi qualche e-mail con allegato infetto, che l'antivirus rileverà e bloccherà. Fine del test.

Se tuttavia siete così fortunati che nessuno vi manda mai virus e volete eseguire un test innocuo dell'efficacia del vostro antivirus, potete usare i "falsi virus" messi a disposizione dalle principali società antivirali e da associazioni di esperti come l'EICAR, presso *www.eicar.org/anti_virus_test_file.htm*.

Si tratta di file **innocui**, che però contengono frammenti di virus resi inoffensivi o altri elementi che il vostro antivirus **deve** riconoscere come pericolosi (come mostrato nella Figura 6.1) anche quando sono all'interno di archivi compressi. Se non li riconosce, c'è qualcosa che non va e vi serve un intervento esperto.

Figura 6.1

*Non usate **mai** un virus vero per collaudare un antivirus. State scherzando con il fuoco.*

Anche questi "falsi virus", comunque, devono essere maneggiati con attenzione. Se li scaricate sul vostro computer, l'antivirus li rileverà e probabilmente vi impedirà di accedervi per cancellarli. Rischiate quindi di trovarvi con un file che è sì innocuo, ma manda nel panico perennemente il vostro antivirus, generando allarmi inutili.

La soluzione a questo problema è semplice: quando scaricate il file di prova, salvatelo su un supporto rimovibile (un dischetto, un CD o simili): in questo modo, a test finito, vi basta estrarre il supporto per rimuovere fisicamente il falso virus.

Occhio agli allarmi-truffa

C'è anche un'altra ragione importante per collaudare il proprio antivirus: per vederne il vero messaggio di allarme (alcuni antivirus hanno più di un messaggio, a seconda delle circostanze).

Molti siti Web, infatti, hanno la fastidiosissima abitudine di includere immagini che sembrano finestre di allarme di Windows o di un antivirus, che vi avvisano che il vostro computer *"potrebbe essere infetto"*, *"sta divulgando un indirizzo IP che potrebbe essere usato per attaccarvi"* e via dicendo.

In realtà queste immagini sono una forma squallida di pubblicità: cliccando sui loro falsi pulsanti non interagite con il vostro Windows o con l'antivirus, ma venite portati al sito del prodotto reclamizzato dal pubblicitario senza scrupoli. La Figura 6.2 mostra un caso in cui l'inganno è smascherato più facilmente del solito, perché la falsa finestra di Windows è addirittura visualizzata su un Mac, le cui finestre di dialogo hanno un aspetto completamente diverso.

Oltre a imparare a riconoscere i messaggi d'allarme autentici del vostro antivirus, c'è un altro trucchetto per non farsi spaventare da questi falsi avvisi: cambiare i colori e i caratteri usati da Windows (*Start* > *Impostazioni* > *Pannello di Controllo* > *Schermo* > *Aspetto*). La falsa finestra di allarme userà molto probabilmente i colori standard e quindi risalterà chiaramente.

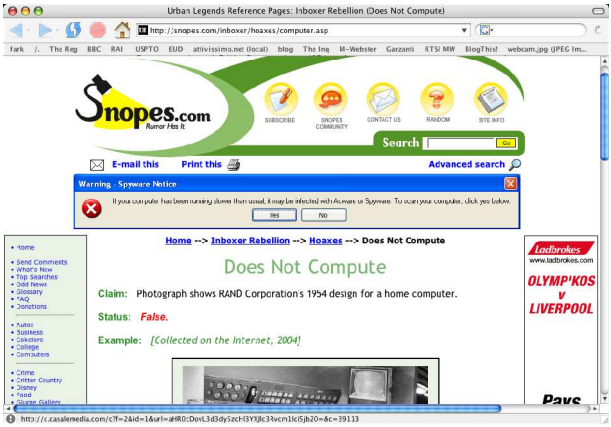

Figura 6.2

Perché tutti mi dicono che sono infetto?

Vi sarà capitato di ricevere **da sconosciuti**, ossia da persone od organizzazioni alle quali non avete mai mandato un e-mail e che magari non avete mai neppure sentito nominare, delle strane **notifiche** secondo le quali avreste inviato a questi sconosciuti dei **messaggi contenenti virus**, anche se siete sicuri di non essere infetti.[50]

Nella maggior parte dei casi potete ignorare questi avvisi. Sono generati per **errore** da programmi antivirus mal configurati dai loro amministratori informatici.

Perplessi? Mi sa che qui ci vuole uno spiegone: arriva subito.

Quando la cura è peggiore del male

Per capire le ragioni di questi falsi avvisi occorre fare un passo indietro. Moltissimi virus attingono alla rubrica degli indirizzi della vittima per trovare nuovi bersagli.

Di conseguenza, capita spesso che un virus infetti il computer di un vostro conoscente, nella cui rubrica trova il vostro indirizzo. Il virus poi confeziona un messaggio infetto usando come falso mittente il vostro indirizzo di e-mail e lo manda a un altro indirizzo, trovato sempre nella rubrica del vostro conoscente infetto.

Purtroppo l'antivirus di chi riceve il messaggio infetto è troppo stupido per rendersi conto che il mittente è stato falsificato, lo prende per buono e quindi genera automaticamente una notifica per avvisare il *presunto* mittente che ha inviato un virus: ma il presunto mittente siete voi, e così la notifica arriva a voi, anziché all'utente effettivamente infetto e responsabile dell'invio.

Confusi? Provo a chiarire con un esempio:

- la vostra amica **Adalgisa** si fa infettare da un virus;
- **Adalgisa** ha in rubrica, fra gli altri indirizzi, il **vostro** e quello di **Bernardo**;
- il virus legge la rubrica di **Adalgisa** e ne estrae il **vostro** indirizzo e quello di **Bernardo**;
- il virus sul computer di **Adalgisa** manda a **Bernardo** un e-mail infetto usando come falso mittente il **vostro** indirizzo;
- l'antivirus di **Bernardo** riceve il messaggio infetto, vede che come mittente è indicato il **vostro** indirizzo e manda **a voi** la notifica;
- **voi** impazzite chiedendovi perché succedono queste cose.

Questo crea confusione pazzesca, panico inutile e un ulteriore traffico di messaggi superflui e ingannevoli che si somma al caos

di messaggi generato dal virus, contribuendo massicciamente a un inutile sovraccarico di e-mail. Praticamente, il traffico raddoppia, dato che questi antivirus generano una notifica per ogni e-mail infetto ricevuto.

Non è raro trovarsi la casella intasata da queste notifiche. La cosa produce non soltanto fastidio, ma anche vere e proprie perdite di tempo, soprattutto quando ricevete richieste d'aiuto da amici non esperti, in preda al panico perché hanno ricevuto una di queste notifiche e temono di essere infetti. Occorre ogni volta fermarsi a spiegare la situazione.

Questi allarmi inutili sono un danno per la Rete e per gli utenti. Lo riconoscono persino i produttori di antivirus,[51] ma i loro prodotti continuano a generarli. Eppure praticamente tutti gli antivirus hanno un'opzione che consente di disattivare l'invio automatico delle notifiche. Evidentemente i responsabili dei sistemi informatici che usano questi antivirus non si rendono conto del danno che provocano con le loro inutili comunicazioni.

> ***Il fatto che quasi tutte queste notifiche siano fasulle non deve indurvi all'imprudenza.*** *L'infezione da virus è sempre in agguato.*
>
> *Rimane comunque* ***indispensabile*** *dotarsi di un buon antivirus e tenerlo costantemente aggiornato, in modo da ridurre al minimo il rischio di essere infetti. In questo modo, quando ricevete una di queste notifiche, potete ignorarla con tranquillità.*

Aiuto! Ho un virus!

Può capitare che nonostante tutto vi prendiate un virus. Succede: il canale d'infezione più frequente in un computer ben blindato è costituito da figli, fratelli e altri animali, che ignorano sistematicamente i consigli e i comportamenti di sicurezza che voi invece seguite così fedelmente. Li seguite, vero?

Normalmente è sufficiente **lanciare l'antivirus e fargli fare una scansione completa del computer**, ma alcuni virus sono in grado di giocare a nascondino e sopravvivere alla pulizia effettuata dall'antivirus, lasciando da qualche parte una propria copia cifrata. Quando riavviate Windows, il virus si ricrea e siete daccapo.

In altri casi, l'antivirus identifica l'infezione ma non riesce a eliminarla. In queste situazioni, ci sono alcuni rimedi che potete tentare, singolarmente o in combinazione, come descritto nelle pagine che seguono.

> *Tenete presente che **disinfestare un computer è un'operazione delicata**. **Se non siete sicuri di quello che state facendo, chiamate un tecnico esperto.** Sono soldi ben spesi, e il fatto di doverlo pagare vi servirà da bruciante promemoria di quanto **prevenire costi meno che curare.***

L'omino delle pulizie

Se il vostro antivirus riesce a identificare un virus ma non riesce a eliminarlo, visitate i siti dei produttori di antivirus e cercate il nome del virus nelle loro enciclopedie virali: troverete quasi sempre istruzioni dettagliate e specifiche su come rimuovere la bestiaccia e probabilmente anche un apposito programma *cleaner*.

Se neppure questo tentativo risolve il problema, usate uno degli antivirus online accennati nelle pagine precedenti e disponibili nei siti dei produttori di antivirus.

Modalità provvisoria

Molto spesso il vostro antivirus riconosce l'infezione ma non riesce a rimuoverla perché Windows non gli consente di accedere ai file infetti. In circostanze come queste c'è un trucchetto che molto spesso risulta decisivo: l'uso della cosiddetta *modalità provvisoria* di Windows.

Questa modalità di emergenza di Windows disattiva tutte le istruzioni eseguite automaticamente all'avvio (comprese quelle eventualmente inserite dal virus per ricrearsi dopo che l'avete cancellato) e carica un Windows "minimo", nel quale potete cancellare a mano i file infetti che prima erano bloccati. Ecco come procedere.

- Prendete nota dei nomi e delle ubicazioni dei file infetti.
- Chiudete Windows e riavviate il computer. Durante il riavvio, quando lo schermo si oscura momentaneamente dopo i primi messaggi diagnostici, premete il tasto F8.

- Windows vi presenta una schermata in cui vi chiede cosa volete fare: premete di nuovo F8 e usate i tasti freccia per evidenziare la voce *Modalità provvisoria*, poi premete Invio due volte.
- Non allarmatevi per le strane scritte che compaiono sul video: è tutto normale.
- Se vi viene proposta la scelta fra utente *Administrator* e il vostro nome, scegliete *Administrator*.[52]
- Compaiono vari promemoria che vi avvisano che siete in modalità provvisoria: accettateli.
- La qualità dell'immagine sullo schermo è minore del solito: anche questo è normale.
- Usate la combinazione di tasti Windows+E per lanciare Esplora Risorse. Sarà probabilmente necessario impostarlo in modo che non nasconda i file, come descritto nel Capitolo 3.
- Cancellate i file segnalati dall'antivirus.
- Provate a lanciare il vostro antivirus: potrebbe non succedere nulla, ma è normale, perché non tutti gli antivirus funzionano nella modalità provvisoria, ma vale la pena di tentare.
- Eseguite il programma *cleaner* specifico per il virus rilevato, se ne avete uno.
- Uscite da Windows e riavviate Windows in modalità normale.

A questo punto l'antivirus non dovrebbe più trovare file infetti.

Niente ripristino, grazie!

Provate a disattivare la funzione *Ripristino configurazione di sistema*, nota anche come *System Restore*, altrimenti Windows potrebbe impedirvi di accedere al file infetto oppure ricreare il virus attingendo alla copia di sicurezza (forse infetta) creata da questa funzione.

- Scegliete *Start* > *Programmi* > *Accessori* > *Utilità di sistema* e lanciate *Ripristino configurazione di sistema*.
- Cliccate su *Impostazioni Ripristino configurazione di sistema* e scegliete la scheda *Ripristino configurazione di sistema*.

- In questa scheda, fate comparire un segno di spunta nella casella *Disattiva Ripristino configurazione di sistema su tutte le unità*.
- Cliccate su OK e rispondete *Sì* alla richiesta di conferma di Windows.
- A questo punto potete lanciare l'antivirus ed eliminare tutti i file che risultano infetti.

> *Ricordatevi poi di riattivare questa funzione una volta debellato il virus!*

Cosa cambia con il Service Pack 2

Il Service Pack 2 non include un antivirus Microsoft, ma si appoggia agli antivirus prodotti da altre società: in altre parole, non vi evita l'incombenza di provvedere alla scelta e all'installazione di un antivirus.

Anzi, mentre prima del Service Pack 2 Windows viveva incurante della mancanza di un antivirus, dopo l'installazione del Service Pack 2 riceverete continui avvisi dal *Centro Sicurezza PC* (la nuova sezione di sicurezza di Windows XP) fino a quando vi deciderete a installare un antivirus. È una funzione chiamata *modalità MQR*, dove MQR sta per *"ma quanto rompi"*.

Il Centro Sicurezza PC (raggiungibile scegliendo *Start* > *Impostazioni* > *Pannello di Controllo* > *Centro sicurezza PC*) riconosce automaticamente gran parte degli antivirus, sia a pagamento sia gratuiti. Se usate un antivirus riconosciuto, il Centro Sicurezza PC vi fa la cortesia di avvisarvi quando si rendono disponibili aggiornamenti per il vostro antivirus e se il vostro antivirus viene disattivato per qualsiasi ragione (per esempio da un virus o da un vostro comando sbagliato).

Se invece adoperate un antivirus diverso da quelli riconosciuti, il Centro Sicurezza PC crede che siate privi di questa protezione vitale e vi tempesta di avvisi. Potete zittirlo cliccando su *Consigli* nel Centro Sicurezza PC e attivando la casella *Si dispone già di un programma antivirus di cui si gestirà il monitoraggio* (Figura 6.3). Naturalmente, dato che usate un antivirus non riconosciuto da Windows, non riceverete avvisi della disponibilità di aggiornamenti o della sua disattivazione.

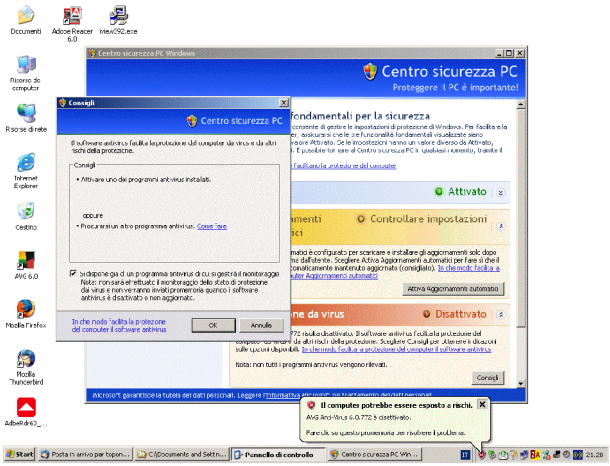
Centro sicurezza PC
Proteggere il PC è importante!
Consigli
Centro sicurezza PC
Attivato
Controllare impostazioni
Disattivato
Il computer potrebbe essere esposto a rischi.

Figura 6.3

Capitolo 7

Spyware: la spia nel computer

I parenti impiccioni dei virus

Come se non bastasse la scocciatura dei virus, ci sono anche degli altri programmi che potreste considerare i cugini ficcanaso dei virus. Non sono ostili in senso informatico, perché non causano al computer devastazioni paragonabili a quelle dei virus e non si propagano automaticamente, ma sono comunque ospiti sgraditi, perché **spiano le vostre navigazioni e le riferiscono ai loro padroni**, sotto forma di dati statistici che non si sa quanto siano anonimi, senza il vostro consenso**.** Questi spioni informatici vanno sotto il nome di *spyware* (si pronuncia *spai-uer*).

Lo spyware si distingue dai virus anche per un'altra ragione: mentre i virus vengono disseminati da criminali e sono universalmente ritenuti illegali, lo spyware viene distribuito molto più alla luce del sole; in molti paesi nei quali le leggi sulla *privacy* sono meno severe che da noi, è considerato addirittura legale.

Questo lo rende in un certo senso più insidioso dei virus, perché lo si può incontrare anche in siti apparentemente rispettabili. Lo spyware si annida in molti dei programmi gratuiti offerti su Internet: giochini, cursori animati, accessori per Internet Explorer e via dicendo. Anche alcuni programmi usati per lo scambio di file (principalmente file musicali) a volte contengono spyware: è il caso, per esempio, di alcune versioni di Kazaa.

Non è finita: oltre allo spyware, ci sono anche altri tipi di programmi-spia ancora più impiccioni: gli *adware*, ossia programmi che vi infettano allo scopo di rifilarvi pubblicità; gli *hijacker*, che dirottano silenziosamente le vostre navigazioni verso siti-trappola; e i *keylogger*, che registrano tutto quello che digitate (comprese le password e i numeri delle carte di credito e le cose indecenti che dite chattando).

I peggiori, comunque, sono i software-spia propriamente detti: quelli che attivano di nascosto microfono e telecamera e permettono al loro padrone di comandare il computer della vittima.

Per semplicità, visto che tutti e tre si combattono usando le stesse tecniche, li raggrupperò sotto il termine più ampio di *spyware*.

Innocuo? Dipende

I danni provocati dallo spyware non si meritano mai un titolo di giornale, ma non sono certo trascurabili. Molti spyware scroccano la vostra connessione a Internet e la rallentano. Alcuni rallentano anche il funzionamento del computer in generale, al punto che un PC infestato da numerosi spyware diventa inutilizzabile.

Ci sono ovviamente anche i danni alla privacy. Una società che vi installa un sistema di monitoraggio o vi rifila pubblicità senza il vostro permesso non è certo molto rispettosa della vostra riservatezza. Vi piace l'idea che qualcuno sappia per filo e per segno che siti avete visitato e quanto tempo vi siete soffermati su ciascuna pagina o immagine?

Non c'è alcuna garanzia che i dati raccolti da questi programmi vengano resi anonimi e non vengano invece rivenduti ad altri commercianti altrettanto disinvolti. Se poi avete a che fare con un *keylogger* che registra tutto quello che scrivete al computer, avete la garanzia contraria: qualcuno userà sicuramente i dati carpiti per fare qualcosa di illecito.

I danni del software-spia vero e proprio possono essere ovviamente micidiali: è come avere un intruso invisibile in casa. Ne vedete un esempio in Figura 7.1: sul PC della vittima è comparsa una finestra di dialogo di Windows, creata in realtà dall'aggressore, la cui traduzione è la seguente:

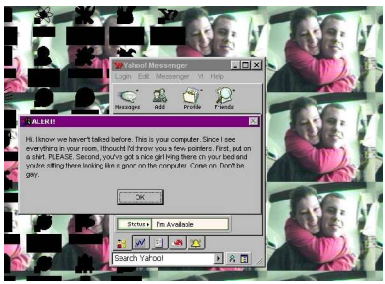

Figura 7.1

"...È il tuo computer che ti parla. Siccome vedo tutto nella tua stanza, ti darei un paio di consigli. Primo, mettiti addosso qualcosa. PER FAVORE. Secondo, hai una bella ragazza sdraiata sul letto e te ne stai seduto lì con una faccia ebete davanti al computer. Dai, non fare il gay".

La Figura 7.2 mostra la comprensibile reazione della vittima.

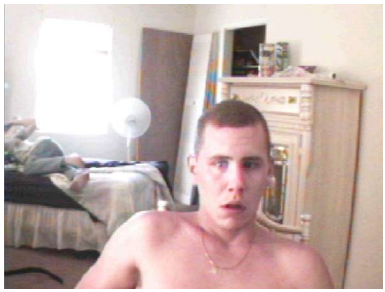

Figura 7.2

Non ridete troppo. Potrebbe capitare anche a voi.

Difendersi dallo spyware

Ci sono quattro consigli fondamentali per difendersi da questi spioni di vario genere.

- **Non usate Internet Explorer** (Regola 6 del Dodecalogo). Quasi tutti gli spyware più subdoli si autoinstallano sfruttando i meccanismi presenti in Internet Explorer. Gli altri *browser* (programmi di navigazione) non hanno questi meccanismi e quindi sono molto più resistenti allo spyware.
- **Non scaricate e non installate software superfluo o di dubbia provenienza** (Regola 5 del Dodecalogo).[53]
- **Se avete una telecamera o un microfono attaccati al computer, copriteli o staccateli fisicamente** quando non li usate. Non fidatevi dei comandi di disattivazione inclusi in Windows: un aggressore li scavalcherà. Se il microfono è integrato, tappatelo oppure inserite uno spinotto nella presa microfonica: disattiverà il microfono interno (Figura 7.3).

- **Usate un antispyware.** Concettualmente analogo all'antivirus, l'antispyware è un programma che esplora il vostro computer alla ricerca di spyware e lo elimina.

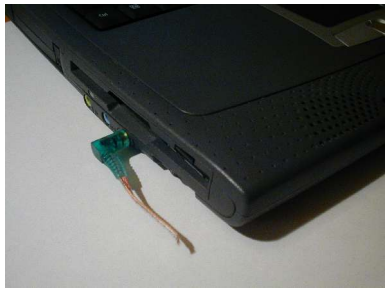

Figura 7.3

Antispyware a scelta

Come per gli antivirus e i firewall, anche per gli antispyware c'è un'ampia scelta, sia a pagamento, sia gratuita. Ecco una breve lista dei più gettonati.

- **Nome:** Ad-Aware
  Produttore e sito: Lavasoft, *www.lavasoftusa.com/default.shtml.it*
  Prezzo: gratuito nella versione base (se per uso personale), a pagamento nelle versioni più complete
  Lingua: multilingue, compreso l'italiano[54]
- **Nome:** PestScan
  Produttore e sito: Zone Labs, *www.zonelabs.com*
  Prezzo: gratuito
  Lingua: inglese
- **Nome:** Spybot Search & Destroy
  Produttore e sito: Patrick Kolla e gli informatici di tutto il mondo, *www.spybot.info/it/index.html*
  Prezzo: gratuito, si accettano donazioni
  Lingua: multilingue, compreso l'italiano
- **Nome:** SpywareBlaster
  Produttore e sito: Javacool Software, *www.javacoolsoftware.com/spywareblaster.html*

Prezzo: gratuito, si accettano donazioni
Lingua: inglese

Attenzione ai programmi antispyware "trovati in giro" su Internet. Molti produttori di spyware cercano di imbrogliare offrendo programmi gratuiti antispyware, che però rimuovono lo spyware che avete nel PC soltanto per sostituirlo con altro spyware, i cui proventi vanno al produttore del falso programma di protezione.

Du antispyware is megl che uan

Diversamente dagli antivirus, che spesso vanno in conflitto fra loro se ne installate più di uno, conviene installare e usare più di un antispyware. Capita infatti abbastanza spesso che un antispyware riesca dove l'altro fallisce o non rileva nulla: il problema dello spyware è molto più sfumato di quello dei virus e ciò che è spyware per alcuni programmi di difesa non lo è per altri.

C'è anche un altro motivo per avere due o più antispyware: alcuni programmi-spia sanno come disattivarli, ma non sempre sanno come disattivarli *tutti*. Raddoppiando gli antispyware, aumentate le probabilità che lo spyware non riesca a disattivare tutte le vostre difese.

Aggiornamenti dell'antispyware

Le analogie fra antivirus e antispyware non sono finite: infatti anche gli antispyware, come gli antivirus, necessitano di aggiornamenti periodici.

Man mano che vengono realizzati nuovi spyware, è necessario aggiornare le "foto segnaletiche" nella memoria dell'antispyware. Per fortuna l'esigenza di aggiornare non è così ossessivamente frequente come capita invece con gli antivirus: se non navigate con browser vulnerabili, non vi capiterà di infettarvi con lo spyware molto spesso, e gli spyware nuovi non nascono con la stessa rapida cadenza che caratterizza i virus.

Come collaudare un antispyware

C'è un modo molto semplice: fategli esaminare il vostro computer. Se non è fresco di installazione, è quasi sicuro che troverà qual-

che spyware. La Figura 7.4 mostra la scansione con Ad-Aware di un computer nuovo di zecca, infettato da uno spyware/adware dopo qualche ora di navigazione non protetta con Internet Explorer.

Secondo una recente indagine di Earthlink.net, la percentuale di PC inconsapevolmente infetta è vicina al 90% e spesso in un medesimo computer coabitano più spyware[55]. Persino Bill Gates ha ammesso di essersi trovato dell'*adware* nei PC di casa.[56]

Figura 7.4

Attenti a falsi allarmi e falsi amici

Una differenza importante fra antivirus e antispyware è che i risultati di un antispyware non sono precisi come quelli di un antivirus. Un virus è un virus, c'è poco da disquisire; ma anche alcuni programmi assolutamente legittimi vengono talvolta identificati come spyware. Alcuni antispyware rilevano anche Internet Explorer come una minaccia, nel senso che contiene delle falle (*exploit*) che consentirebbero a un programma-spia di infettarvi (Figura 7.5).

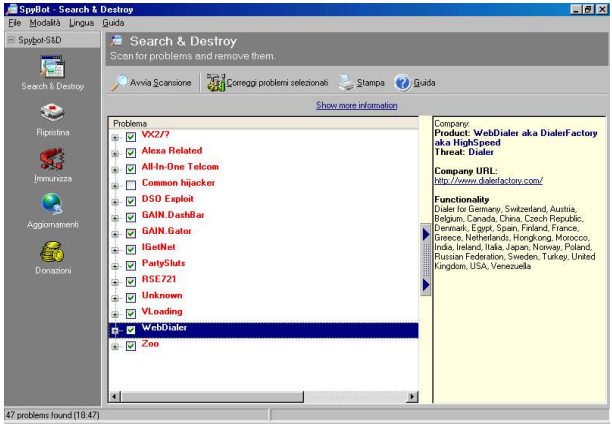

Figura 7.5

Ci vuole insomma un po' di cautela prima di assecondare le segnalazioni di un antispyware e cancellare i file considerati a rischio. La maggior parte degli antispyware tiene conto di quest'esigenza di cautela e infatti non cancella automaticamente i file sospetti, ma si limita a segnalarli e vi offre di metterli in una sorta di "cella di isolamento", dalla quale potete tirarli fuori se vi rendete conto che vi servono.

C'è un'altra ragione per cui conviene riflettere prima di cancellare un file segnalato dall'antispyware: rimuovendo lo spyware, il programma che lo contiene smette di funzionare. È il caso, per esempio, di vari "ausilii di navigazione" per Internet Explorer e di alcuni programmi per lo scambio di file. A voi la scelta: o vi tenete il programma insieme allo spyware, o buttate via entrambi.

E se lo spyware non se ne va? Ogni tanto l'antispyware deve arrendersi: segnala un problema ma non riesce a eliminarlo. In casi come questi, conviene usare le stesse tecniche seguite per i virus: provate un altro antispyware, oppure usate la *modalità provvisoria*, descritta nel Capitolo 6.

Rischi assortiti

I moderni antispyware contengono molte funzioni di difesa supplementari, oltre al semplice rilevamento dei programmi-spia. Per esempio, molti antispyware sono in grado di bloccare il file *hosts*,

che alcuni aggressori modificano in modo da imbrogliare Windows e costringervi a passare attraverso i loro siti quando navigate.

Un'altra funzione molto utile degli antispyware è la protezione della pagina iniziale di Internet Explorer. Una delle lamentele più frequenti di chi usa Windows è la comparsa del tutto inattesa e indesiderata di una pagina Web di un sito pornografico appena si avvia Internet Explorer. Questo avviene perché alcuni spyware e virus sono in grado di reimpostare la pagina inizialmente visualizzata in Internet Explorer. Gli antispyware bloccano questi tentativi di reimpostazione.

Gli antispyware sono anche molto efficaci contro un'altra minaccia presente su Internet: i *dialer*, ossia i famigerati programmi che causano addebiti da infarto sulla bolletta telefonica. Ve ne parlo nel prossimo capitolo.

Capitolo 8

Dialer: i succhiasoldi

Cos'è un *dialer?*

Un *dialer* è un programma che **altera i parametri della vostra connessione a Internet**, cambiandone il numero telefonico e sostituendolo con un **numero a pagamento maggiorato** su prefissi come il costosissimo **899** o su prefissi internazionali. Parte di quello che si paga per queste telefonate viene girato dall'operatore telefonico a una terza persona o società: quella che appunto dissemina i dialer, con guadagni da capogiro.

Per esempio, il virus-dialer *Zelig*, diffusosi nell'Internet Italiana a ottobre 2003, fruttò in meno di un mese scatti rubati per oltre 104.000 euro (ma anche una condanna al suo ideatore).[57]

Il dialer sarebbe di per sé uno strumento lecito del commercio via Internet. Per esempio, una società potrebbe usarlo per offrire consulenze o informazioni per telefono e farsi pagare per questi servizi direttamente tramite la bolletta del chiamante, senza dover scomodare carte di credito, fatture e quant'altro.

Purtroppo, però, è uno strumento largamente abusato, nel senso che viene offerto spessissimo facendo di tutto per nascondere i veri costi di connessione, che possono arrivare **anche a centoquaranta euro l'ora**. I siti truffaldini usano giri di parole come *"0,041 euro al secondo"*, che non rendono affatto l'idea che si tratta di **due euro e passa al minuto.**

I dialer non sono relegati nel sottobosco dei siti pornografici: **potete trovare un dialer ovunque**, anche in siti apparentemente rispettabilissimi. Alcuni siti "sparadialer" offrono infatti ricette, musica, suonerie, aiuti per la maturità scolastica o informazioni turistiche.

Trucchi dei dialer

La maggior parte dei dialer agisce tramite il cosiddetto *"avviso di protezione"* (Figura 8.1): una finestra di avviso che molti interpretano come un "certificato di garanzia" del dialer.

In realtà, il senso di questo messaggio di Windows è un altro: *"state per installare un programma che potrebbe anche danneggiare il computer: siete davvero sicuri di voler correre questo rischio?"*.

Figura 8.1

I dialer ricorrono anche ad altri espedienti per non far capire che si tratta di connessioni su tariffa 899 e simili: per esempio, i parametri della loro connessione, nella sezione Accesso Remoto di Windows, spesso non visualizzano il numero composto.

> *Tutte le volte che vedete una finestra di dialogo del tipo mostrato in Figura 8.1,* ***fermatevi*** *e chiedetevi se il sito che state visitando ha una buona ragione per obbligarvi a installare qualcosa. Se non è un sito di indubbia affidabilità (la vostra banca o Microsoft, per esempio), potreste essere a un passo dall'infettarvi con un dialer.* ***Se siete alle prese con un dialer e cliccate su Sì, vi infetterete****.*

L'avviso di protezione non è l'unico metodo usato per infettarvi con un dialer: per esempio, alcuni siti vi chiedono esplicitamente di scaricare ed eseguire *"un piccolo programma GRATUITO"* che permetterà di accedere ai loro "servizi particolari", contando sul fatto che la parola *"GRATUITO"* in maiuscolo distrarrà dalla lettura dei veri costi del servizio. Il bello è che questi siti non mentono,

perché **il programma in sé è in effetti gratuito: è la *telefonata* che costa carissima**.

Oltre a questi metodi artigianali, i dialer approfittano anche di alcune vulnerabilità dei programmi più diffusi (Internet Explorer e Outlook Express) che consentono a un sito o a un utente ostile di indurre il computer della vittima a scaricare ed eseguire un programma (in questo caso il *dialer*) senza che l'utente se ne accorga e spesso senza che l'utente faccia altro che visualizzare senza protezione un e-mail o una pagina Web appositamente confezionata.

> *Molte di queste tecniche di attacco **non sono rilevabili dai comuni antivirus** (perché appunto non sono virus), per cui la presenza dell'antivirus aggiornato sul vostro computer non deve darvi una sensazione di falsa sicurezza.*

Come difendersi

Come al solito, la prevenzione è la soluzione più efficace: ci si può sbarazzare dei dialer e contenerne gli effetti anche dopo che si sono insediati, ma è un'impresa molto più impegnativa che evitarli in partenza.

Non usare Internet Explorer e Outlook Express

Usare browser diversi da Internet Explorer è la migliore forma di prevenzione. Quasi tutti i siti sparadialer, infatti, ricorrono al trucco degli avvisi di protezione, che **funzionano soltanto con Internet Explorer** e i browser basati su Internet Explorer: pertanto, se visitate un sito sparadialer con un altro browser, non li vedrete neppure e non potrete scaricarli neppure volendo.

Altri dialer arrivano come allegati ai messaggi di posta, e se usate Outlook Express o altri programmi che si appoggiano a Internet Explorer per visualizzare i messaggi, correte il rischio di infettarvi automaticamente.

Conviene pertanto non usare Outlook Express o perlomeno impostarlo in modo che non visualizzi i messaggi tramite Internet Explorer e non esegua eventuali comandi nascosti, come descritto nei Capitoli 11 e 12. Il problema dei dialer è una delle tante moti-

vazioni della Regola 6 del Dodecalogo che sconsiglia appunto l'uso di Internet Explorer e Outlook Express.

Con un browser alternativo, invece, l'unico modo per subire i danni di un dialer è scaricare ed eseguire *intenzionalmente* un programma da un sito di cui non conoscete la reputazione. Non è impossibile, ma è molto meno probabile.

Usare antispyware e antidialer

Alcuni programmi per la difesa dallo spyware sono in grado di riconoscere anche i dialer: tenere un antispyware in funzione, in modo che sorvegli costantemente il funzionamento del PC, è quindi una buona forma di prevenzione, perché consente di bloccare il dialer prima che si installi nel vostro computer.

Inoltre, come se non bastassero antivirus e antispyware, ci sono anche gli *antidialer*: programmi che sorvegliano la connessione telefonica a Internet e bloccano eventuali tentativi di modificarla.

C'è per esempio un programma gratuito, *Stop Dialers* di Giulio Bottini, scaricabile presso *www.socket2000.com*: impostate il numero telefonico della normale connessione a Internet che volete usare e poi lasciate che Stop Dialers faccia il resto. Se un dialer vi infetta, perlomeno non riuscirà a cambiare il numero di telefono composto dal modem.

Passare alla banda larga

I dialer funzionano soltanto sulle connessioni effettuate tramite modem su linea telefonica ordinaria. Pertanto, attivare un abbonamento ADSL o su fibra ottica (la cosiddetta *banda larga*) è una soluzione perfetta al problema, perché vi fa cessare di usare il modem sulla normale linea telefonica.

Questo non significa che non potete più infettarvi: vuol dire semplicemente che se vi infettate con un dialer, non subirete addebiti in bolletta.

*Quando passate alla banda larga, **ricordatevi di scollegare il modem per linee telefoniche ordinarie** che avete usato fino a quel momento. Meglio ancora, se avete un modem rimovibile, toglietelo direttamente dal computer. Così al dialer mancherà fisicamente la linea da sfruttare.*

*Fate molta attenzione se usate il PC come segreteria telefonica o come fax: in questi casi, infatti, lasciate il modem telefonico collegato anche alla normale presa del telefono e quindi **rimanete vulnerabili ai dialer.***

Anche se passate alla banda larga, **i dialer possono comunque fare talvolta un piccolo danno: far cadere la connessione**, soprattutto se il vostro collegamento ADSL usa un modem collegato alla porta USB del computer.[58] Questo non provoca addebiti in bolletta, ma è comunque una scocciatura, specialmente se capita mentre state scaricando un file molto grande.

Bloccare i prefissi usati dai dialer

Potete rivolgervi a Telecom Italia, al 187, per far disabilitare gratuitamente l'accesso a tutti i prefissi nazionali usati dai dialer, ossia 144, 166, 709 e 899. Con la stessa richiesta, e altrettanto gratuitamente, potete far bloccare anche i prefissi satellitari e quelli internazionali della cosiddetta "Zona 7", che comprendono i prefissi 0088 e 0068 usati da certi dialer. Queste disabilitazioni non impediscono le altre chiamate: tutti gli altri prefissi internazionali restano accessibili.[59]

In questo modo, se anche venite infettati, il dialer non riuscirà a fare alcuna chiamata e quindi non andrete incontro a salassi in bolletta. Sulla bolletta troverete soltanto un promemoria che indica lo stato della disabilitazione.

Lo stesso discorso vale anche per gli altri operatori, che per legge devono fornire gratuitamente la disattivazione di questi prefissi.[60]

Aggiornare Windows

Molte delle falle di Windows che permettono ai dialer di colpirvi sono già state corrette da Microsoft tramite gli aggiornamenti che potete installare tramite la voce *Windows Update* del menu Start.

In particolare, c'è un aggiornamento molto importante, denominato *Service Pack 2*, che tura un gran numero di queste falle e rende molto meno vulnerabile Internet Explorer e il resto di Windows, soprattutto per quanto riguarda la trappola degli avvisi di protezione: vengono bloccati salvo vostro contrordine.

Assicuratevi di installare questo Service Pack 2 e tutti gli aggiornamenti definiti "critici" da Microsoft, con le cautele descritte in dettaglio nel Capitolo 10.

Verificare la presenza di un dialer

Esiste un metodo estremamente semplice per sapere se siete stati colpiti da un dialer: aspettare la bolletta. Garantisco che ve ne accorgerete subito anche se non siete dei geni dell'informatica.

Se preferite un metodo meno cruento, c'è un sistema rozzo ma efficace per controllare che numero viene *effettivamente* composto dal vostro modem: impostare il modem in modo che si sentano i toni di composizione del numero e inserire una virgola nel numero.

I toni del modem si attivano in questo modo:

- *Start* > *Impostazioni* > *Pannello di controllo* > *Opzioni modem e telefono:* scegliete la scheda Modem.
- Selezionate il modem e cliccate su *Proprietà*, poi scegliete la scheda Modem.
- Regolate il cursore del volume dell'altoparlante.

La virgola si imposta invece scegliendo *Start* > *Impostazioni* > *Connessioni di rete* e la connessione al vostro fornitore d'accesso a Internet e poi immettendo la virgola nel numero indicato nella casella *Componi*.

Secondo le arcane regole della tecnologia dei modem, la virgola fa fare una pausa durante la composizione del numero. In questo modo, se vi collegate a Internet e non sentite la pausa nella "musichetta" dei toni di composizione, il numero effettivamente composto non è quello che avete scelto voi e quindi potreste essere infettati da un dialer. Se invece sentite la pausa, il numero composto è davvero quello che avete richiesto.

Contrariamente a quanto potreste pensare, ***non è sufficiente guardare nelle impostazioni del modem e***

***vedere che numero di telefono contengono**. Alcuni dialer, infatti, sono abbastanza astuti da lasciare inalterate queste impostazioni ma subentrare con le loro impostazioni quando lanciate la connessione a Internet. Altri dialer non visualizzano assolutamente nulla nella finestra di Accesso Remoto.*

Addebito in bolletta, che fare?

Se un dialer vi ha già colpito e quindi avete verificato la presenza di un dialer nel peggiore dei modi possibili, contattate subito un'associazione di consumatori per sapere quale strategia adottare. Telecom Italia, infatti, sta cambiando atteggiamento nei confronti delle vittime dei dialer. Che sono veramente tante: nel 2003 sono state fatte oltre duecentomila denunce per questo fenomeno.

Dopo un periodo in cui la procedura standard era pagare la parte non contestata della bolletta e avviare una procedura di conciliazione, dall'inizio del 2004 l'operatore telefonico sembra infatti incline a esigere comunque il pagamento integrale della bolletta e alcune sentenze recenti sembrano dargli ragione.[61] La denuncia presso il più vicino Ufficio di Polizia Postale e delle Comunicazioni o qualunque altro Ufficio di Polizia è ancora possibile, naturalmente, ma non consente di sospendere il pagamento delle bollette.

In sintesi: prevenire (con il blocco dei prefissi usati dai dialer) è facile, curare (nel senso di non dover pagare l'addebito) è un'impresa quasi disperata. Quindi posso soltanto consigliare di prevenire il problema attivando **subito** il blocco gratuito dei prefissi incriminati.

Si può denunciare questa gentaglia?

Dipende. Se il dialer non dichiara i costi, si può fare segnalazione di pubblicità ingannevole all'Autorità per le Garanzie nelle Comunicazioni. L'indicazione **chiara** dei costi, infatti, è un obbligo di legge.

Se il sito sparadialer contiene materiale pornografico e il dialer usa i prefissi nazionali 899, 144 e 166, è denunciabile alla Polizia di Stato anche se non vi ha causato alcun addebito: infatti i servizi dal contenuto erotico, osceno o pornografico su questi numeri sono esplicitamente vietati dal decreto legge 23 ottobre 1996,

n.545, convertito dalla legge 23 dicembre 1996. Questo divieto non si applica ai servizi che usano numerazioni internazionali.

Trovate maggiori informazioni e indirizzi da contattare presso questa pagina del sito della Polizia di Stato: *www.poliziadistato.it/pds/primapagina/899/899.htm*. Potete dare anche voi una mano a tenere pulita la Rete.

Capitolo 9
Backup

L'ultima linea di difesa

Non lasciatevi ingannare dal fatto che questo capitolo è a metà del libro: la copia di sicurezza, ossia il *backup*, non è da considerare meno importante di tutto quello che avete letto sin qui. Anzi, il backup è la vostra estrema linea di difesa quando tutto il resto va a ramengo e avete il computer infetto da un virus e/o devastato da un intruso.

Ebbene sì, queste cose possono capitare nonostante tutte le precauzioni, semplicemente perché la sicurezza non è un concetto assoluto e soprattutto perché l'errore umano è sempre in agguato, magari sotto forma di un allegato che ci sembra troppo interessante (per esempio *annakournikova.jpg.vbs*) per non aprirlo subito, senza controllarlo prima con l'antivirus aggiornato e comunque lasciarlo in quarantena, o sotto forma di figli, fratelli, coniugi o genitori che smaniano di installare la copia pirata dell'ultimo giochino, fornitagli da chissà chi.

Bisogna anche considerare la possibilità, niente affatto remota, di un aggiornamento infelice dei programmi o dei componenti del computer, oppure di un guasto ai suoi componenti fisici. Un fulmine che entra nell'impianto elettrico, il normale invecchiamento del disco rigido, una caduta o un gesto maldestro possono danneggiare irreparabilmente il computer e rendere inaccessibili i vostri dati anche senza lo zampino di un aggressore.

In queste circostanze, soltanto il backup vi permetterà di ripristinare il computer (o almeno i vostri dati) alle condizioni precedenti il disastro. Se non avete il backup, nella migliore delle ipotesi potete tentare una onerosissima pulizia, che non ha garanzie assolute di successo e richiede molta pazienza e abilità; nella peggiore, avete perso tutto: foto, musica, documenti, corrispondenza, contabilità. Con il backup evitate tutte queste ansie e tribolazioni.

Ecco perché la Regola 3 del Dodecalogo è così perentoria:

Regola 3: Fate il backup (almeno) dei vostri dati. Fatelo spesso. Fatelo SEMPRE!

Backup, l'oggetto misterioso

Sarà il termine straniero, sarà l'incoscienza che fa pensare *"tanto a me non succede"*, sarà quel che sarà, ma il backup è il più trascurato e incompreso degli strumenti di difesa informatica. Come una vaccinazione, sembra una precauzione superflua e ci si accorge quanto sia utile soltanto nel momento del bisogno.

Eppure un backup non è nulla di trascendentale: è semplicemente **una copia in più dei vostri dati più preziosi**, fatta quando li aggiornate. Al livello più semplice, per fare un backup basta prendere un file che volete evitare di perdere in caso di problemi e copiarlo altrove: in un'altra cartella del computer, su un dischetto, su un CD, su un DVD o un qualsiasi altro supporto. Tutto qui.

Naturalmente il backup può anche essere un affare più complesso, altrimenti questo capitolo sarebbe già finito. Per esempio, non è sempre facile accorgersi che un file è stato aggiornato e quindi ha bisogno di un backup.

Quando modificate un documento (un testo, una foto, una registrazione audio o video, per esempio), è ovvio che ve ne accorgete. Ma Windows e i suoi programmi spesso aggiornano dei file "dietro le quinte". L'archivio dei messaggi di posta, per fare giusto un esempio, viene aggiornato quotidianamente, ed è contenuto in uno o più file. Anche i parametri di configurazione dei programmi sono memorizzati in file nascosti chissà dove sul disco rigido. Windows aggiornerà questi file senza avvisarvi.

In altre parole, non basta fare una copia di backup dei file che *sapete* di aver aggiornato. Per poter ripristinare la situazione com'era, bisogna fare un backup anche dei file aggiornati da Windows "di nascosto". Per fortuna ci sono appositi programmi di backup, che automatizzano il procedimento e sono in grado di identificare tutti i file aggiornati (da voi o da Windows) e poi generarne una copia di scorta.

Ma un backup può fare anche di più: può riparare il funzionamento di Windows. Capita piuttosto spesso che a furia di installare e disinstallare programmi, Windows vada in tilt, o che un virus si intru-

foli in un momento in cui avete abbassato la guardia e non si riesca a eliminarlo, con il classico risultato che ogni volta che avviate il PC vi compare di fronte un turgido quanto imbarazzante ammasso di carne e silicone in pose inequivocabili. In tal caso c'è quasi sempre una sola strada: azzerare il disco rigido e reinstallare pazientemente Windows e poi tutti i programmi, uno per volta, con le relative impostazioni personalizzate. Uno strazio.

La sofferenza si attenua parecchio, però, se avete creato un **backup dell'*intero contenuto*** del disco rigido (Windows, programmi e dati) prima del tilt: in tal caso, vi basta azzerare il disco e poi copiarvi sopra il backup integrale per riottenere il computer esattamente com'era prima del disastro, con tutte le installazioni e configurazioni già fatte.

A quest'incombenza provvede un'apposita categoria di programmi di backup, che invece di salvare singoli file creano le cosiddette *immagini*: una sorta di "fotocopia" esatta dell'intero disco rigido del computer, trasferibile su CD o DVD o altro supporto.

Ma devo proprio?

A seconda dell'uso che fate del computer e dell'importanza dei dati che gli affidate, la necessità di effettuare i vari tipi di backup può variare drasticamente. Per esempio, se avete tempo da vendere e non vi dispiace correre il rischio di passare un fine settimana a reinstallare tutto da capo, potete fare a meno del backup integrale a immagini.

Il backup dei dati è un altro paio di maniche: da quello non si scappa. Se non lo fate, prima o poi ve ne pentirete. Anche in assenza di attacchi, i computer si guastano, e lo fanno sempre nel momento peggiore. Ho assistito a tante scene di disperazione di utenti che si sono resi conto di aver perso *anni* di ricordi (musica, foto, documenti, numeri di telefono, tesi di laurea): vorrei risparmiarvi questa sofferenza.

Beh, io vi ho avvisato: se ignorate questa raccomandazione, non venite a piangere da me.

Va bene, va bene... ma *quanto* spesso?

L'esatto significato di *"spesso"* varia da persona a persona e da situazione a situazione. Il criterio fondamentale è questo: **quante**

ore (o giorni) di lavoro al computer sareste disposti a rifare? La cadenza dei backup deve essere più ravvicinata di quel periodo di perdita sopportabile.

Se state lavorando a una tesi o a un documento vitale per il vostro lavoro, per esempio, vi conviene fare il backup di quel documento anche più volte al giorno, magari semplicemente salvandolo con nomi diversi e progressivi, tipo *Cura per i peli superflui1.doc*, *Cura per i peli superflui2.doc* e così via, salvandone l'ultima versione su un altro supporto a fine giornata.

Inoltre il backup va fatto **prima di ogni modifica al computer**: in altre parole, prima di installare o rimuovere programmi, prima di installare aggiornamenti del sistema operativo e prima di installare o rimuovere componenti e accessori (stampanti, schede, memoria, eccetera) del computer.

E dove lo scrivo?

Per quanto riguarda i supporti su cui scrivere le copie di backup, avete soltanto l'imbarazzo della scelta e non dovete temere costi insostenibili.

- Per i backup di singoli documenti, potete usare un **dischetto** oppure una più capiente **memoria USB**. Ormai quasi tutti i documenti moderni sono troppo grandi per stare su un dischetto, per cui vi conviene investire in uno di questi praticissimi aggeggi, grandi come un evidenziatore, che si collegano alla porta USB di qualsiasi computer, compresi Mac e Linux, e sono capienti come qualche centinaio di dischetti (Figura 9.1). Non ve ne pentirete.

Figura 9.1

- Per i backup di grandi quantità di dati (un archivio di posta, una raccolta di qualche anno di foto, la vostra musica preferita), vi serve un supporto molto capiente: di solito la scelta cade su un **CD o DVD**. Questi supporti sono fra l'altro immuni ai normali campi magnetici, a differenza del disco rigido.
- Per grandissime quantità di dati (diversi gigabyte) e per i backup-immagine completi, vi occorre un supporto ancora più capiente: di solito si usa un **disco rigido supplementare**, che può essere interno al computer, collegato come accessorio esterno, oppure situato in un altro computer collegabile tramite una connessione di rete locale.

Riciclaggio

Potete contenere drasticamente i costi di backup ricorrendo a un classico trucco: **riciclare i vecchi backup**. Se usate supporti riscrivibili (compresi CD e DVD), potete creare un certo numero di backup consecutivi e poi scrivere ogni nuovo backup sui supporti usati per il backup più vecchio.

Per esempio, immaginate di prendere tre CD riscrivibili e di fare backup giornalieri. Lunedì usate il primo CD, martedì il secondo, mercoledì il terzo; giovedì riusate il primo, venerdì il secondo e così via. Se prevedete la necessità di tornare a backup risalenti a più di tre giorni prima, vi basta aumentare il numero di CD della serie.

Fatelo SEMPRE!

È facile adagiarsi e cominciare a pensare *"tanto oggi cosa vuoi che succeda"* e smettere di fare il backup regolarmente. Ed è proprio allora, in ossequio alle celebri leggi di Murphy, che la sfiga (che notoriamente ci vede benissimo) vi colpirà implacabilmente.

Io ne so qualcosa; i backup quotidiani di tutti i miei dati mi hanno salvato in tante occasioni da disastri sia a livello professionale (perdita di lavoro) sia a livello personale (diari, dati, foto, appunti, filmati che altrimenti avrei perso per sempre).

Vi garantisco che non c'è niente come far cadere un laptop appena prima di un viaggio di lavoro per apprezzare l'utilità di un backup. In quell'occasione, corsi a comperare un nuovo portatile, vi

reinstallai il software e ripristinai tutti i dati, compresi quelli della ricerca che dovevo presentare durante il viaggio, e mi salvai da una figuraccia galattica.

E mi raccomando: **collaudate periodicamente i backup**. Può capitare che ci sia un errore di scrittura o di procedura, per cui il backup sembra essere stato creato regolarmente ma in realtà è inservibile o non include tutti i file che vi servono. Provate ogni tanto a ripristinare qualche file e vedere che succede.

Scoprirete, fra l'altro, che il backup vi permette di recuperare i file che immancabilmente capita di cancellare per poi rendersi conto di averne bisogno... ovviamente un istante dopo aver vuotato il Cestino di Windows.

Scegliere un programma di backup

Non è detto che dobbiate affrontare una spesa per procurarvi un programma di backup. Windows include già un semplice programma di questo tipo, sufficiente per le situazioni normali. Se avete un masterizzatore, nel CD di programmi che l'accompagna c'è spesso anche un programma di backup. Inoltre molti validissimi programmi di backup sono scaricabili gratuitamente da Internet.

Backup semplice semplice con Esplora Risorse

Se volete salvare soltanto qualche file ogni tanto, non vi serve un programma apposito: vi basta usare Esplora Risorse. Copiate i file al supporto esterno e avete finito.

Esplora Risorse può essere sufficiente anche per backup un po' più estesi. Se siete tipi ordinati e riuscite ad addomesticare Windows e i suoi programmi in modo che salvino tutti i loro dati e parametri di configurazione dentro cartelle contenute in una cartella principale (chiamatela per esempio *c:\Dati*), invece di disseminarli nel disco come fanno di norma, vi basta usare Esplora Risorse per copiare quella cartella principale.

Tuttavia quest'opera di "addomesticamento" richiede che modifichiate a mano la configurazione dei singoli programmi e di Windows, per cui vi conviene affrontarla soltanto se siete davvero taccagni ma avete molto tempo a disposizione e sapete dove mettere le mani.

In alternativa, potete usare la funzione *Cerca* di Windows (Start > Cerca > File o cartelle) e cercare tutti i file la cui data di modifica è successiva a quella dell'ultimo backup che avete eseguito. Questo vi consente di scoprire tutti i file modificati da voi o da Windows. Selezionateli dall'elenco risultante, copiateli a un supporto esterno e il gioco è fatto.

Backup semplice in Windows XP

Per motivi incomprensibili, nella versione di base di Windows XP, chiamata *Home Edition*, Microsoft include un semplice programma di backup sul CD di installazione, ma non lo installa automaticamente e non lo elenca neppure fra le opzioni di installazione nel Pannello di controllo.

È un controsenso, quasi che Microsoft sottintenda che gli utenti domestici non hanno nulla che valga la pena di salvare in copia. Gli utenti di XP Home devono installare il software manualmente. Ecco come procedere:

- Inserite il CD di Windows e andate nella cartella *\valueadd\msft\ntbackup.*

  Se non trovate una cartella con questo nome, probabilmente avete un cosiddetto CD di recovery di Windows*, ossia un disco che consente di reinstallare Windows soltanto sul computer con il quale è stato venduto. In tal caso vi conviene contattare il vostro rivenditore per farvi spiegare come procedere nel caso specifico. L'uso del programma di backup è un vostro diritto: l'avete pagato nel prezzo d'acquisto del computer.*

- Fate doppio clic sul file *ntbackup.msi* per lanciare il programma di installazione.
- A fine installazione, trovate una nuova voce *Backup* in *Start > Programmi > Accessori > Utilità di sistema.*

Lanciando Backup, parte una procedura guidata, nella quale vi basta scegliere l'opzione più adatta alla vostra situazione (di solito è *Documenti e impostazioni*) e un supporto sul quale scrivere il backup, che è un unico grande file. Tenete presente che anche in un computer fresco di installazione, Backup troverà moltissimi file da

salvare in copia, per cui non dategli un dischetto: fornitegli un supporto più capiente.

Lo stesso programma viene usato per *ripristinare* i dati di cui avete creato un backup: potete scegliere fra ripristinare tutto oppure ripristinare soltanto un file specifico.

Backup integrale

Reinstallare e riconfigurare da capo Windows e tutti i programmi in caso di disastro ha i suoi vantaggi, perché consente di fare un bel repulisti (della serie "il fuoco purifica"). Un Windows fresco di installazione è notoriamente più vispo e agile di un Windows nel quale si sono accumulati i residui di tante installazioni e disinstallazioni di programmi.

Se però volete evitare la sofferenza di una reinstallazione e riconfigurazione del genere, che richiede tempo e pazienza in dosi da fachiro, potete fare una copia di backup dell'intero contenuto del computer, compresi il sistema operativo e i programmi installati e tutte le loro personalizzazioni, usando per esempio questi programmi:

- *Norton Ghost* (*www.symantec.com*), a pagamento.
- *Truelmage* (*www.acronis.com*), a pagamento, con versione di prova scaricabile gratuitamente.
- *Partimage* (*partimage.org*), gratuito.
- Anche il già citato programma *Backup* incluso in Windows offre l'opzione del backup integrale, chiamato *copia replicata*.

I programmi di backup integrale seguono quasi tutti lo stesso principio generale di funzionamento: avviano un mini-sistema operativo alternativo (da dischetto, da CD o da un'area riservata del disco rigido), scavalcando completamente Windows, e creano su un supporto separato un unico grande file, eventualmente divisibile in più parti, contenente l'immagine esatta dell'intero disco rigido.

Se si rende necessario un ripristino integrale di Windows, avviate il computer usando il dischetto di avvio generato appositamente dal programma di backup e fornitegli le coordinate del file contenente il backup. In pochi minuti riavrete il vostro computer esattamente com'era prima del disastro. Bello, vero?

Fra l'altro, si può creare un'immagine del disco rigido anche senza usare un supporto separato: questo risulta utile particolarmente nel caso dei PC portatili, ai quali è talvolta difficile collegare masterizzatori di CD o dischi rigidi esterni.

Il trucco consiste nel dividere preventivamente il disco rigido in due sezioni, denominate *partizioni*, e di mettere tutto (sistema operativo, programmi e dati) in una sola delle partizioni. In questo modo, il programma di backup crede che abbiate *due* dischi rigidi e vi offre la possibilità di fare il backup di uno sull'altro.

> ***Attenzione:*** *creare le partizioni è un'operazione delicata che richiede la mano ferma di un esperto e può comportare la perdita totale dei vostri dati. Non provateci da soli se non siete molto sicuri di quello che fate.*
>
> *Inoltre tenete presente che se si guasta il disco rigido, perderete probabilmente tutte le partizioni e quindi anche il backup. Ricordate quindi di copiare il backup a un supporto esterno, magari tramite una piccola rete locale.*

Punti di ripristino

Windows XP ha anche un altro modo di fare un backup di se stesso, che va sotto il nome di *punto di ripristino* o *punto di arresto del sistema*.

In pratica, in occasione di cambiamenti importanti dello stato del computer, per esempio quando installate un programma o modificate le impostazioni di Windows, potete creare una copia dei file vitali del sistema e dei vostri file personali. Spesso Windows provvede automaticamente a quest'incombenza. Se qualcosa va storto, potete riportare rapidamente il computer a com'era quando avete creato il punto di ripristino.

Il vantaggio di questo metodo rispetto al backup integrale a immagine è che vengono salvati in copia soltanto alcuni file particolarmente importanti, invece di tutti i file, per cui la creazione di un punto di ripristino è in genere molto più rapida di un backup integrale. Inoltre non è necessario il riavvio di Windows richiesto da quasi tutti i programmi di backup integrale e il backup può risiedere sullo stesso disco rigido sul quale risiedono Windows e i vostri dati.

Il programma che gestisce questi punti di ripristino è sotto *Start* > *Programmi* > *Accessori* > *Utilità di sistema* e si chiama *Ripristino configurazione di sistema*.

Per creare un punto di ripristino, lanciate il programma e scegliete (indovinate un po') *Crea un punto di ripristino*. Dategli un nome e il gioco è fatto.

Per ripristinare il computer a uno stato precedente, lanciate ancora il programma e scegliete *Ripristina uno stato precedente del computer.* Scegliete dal calendario a video la data alla quale vi interessa ritornare e lasciate che Windows si riavvii. Vedrete la schermata *Ripristino configurazione di sistema*, e a riavvio completato Windows sarà com'era alla data che avete scelto.

Backup del Registro

Windows e i programmi memorizzano moltissimi parametri di funzionamento in un unico file, denominato *Registro*. Se avete la sensazione che salvare tutto in unico file sia furbo come mettere le proverbiali uova tutte nello stesso proverbiale paniere, avete perfettamente ragione e avete capito una lezione che i progettisti di Windows si ostinano a ignorare: basta che un programma qualunque acceda maldestramente al Registro e non funziona più niente.

Peggio ancora, il Registro diventa un bersaglio ideale per i creatori di virus, che vi insediano le proprie pestifere creature. Potete anche individuare il file che contiene il virus che vi tormenta e cancellarlo, ma se il virus ha iniettato nel Registro un'istruzione che ricrea l'infezione, non ve ne libererete facilmente. Il Registro, insomma, è il ventre molle di Windows.

Anche se non fate un backup completo del sistema operativo, per difendersi dagli attacchi informatici (ricordate che può bastare una semplice visita a un sito Web) conviene insomma creare spesso una copia di sicurezza del Registro.

Per fortuna non occorre imparare un'ennesima tecnica di backup: la creazione di un punto di ripristino include anche una copia del Registro. In alternativa, si può usare il programma Backup di Windows scegliendo, nella modalità avanzata, il backup guidato e l'opzione *Backup solo dello stato del sistema*, che include una copia del Registro.[62]

Il tempo di un caffè

Molti utenti sono riluttanti a gestire i backup perché credono che richiedano troppo tempo. In realtà un punto di ripristino o un backup dello stato del sistema richiedono un paio di minuti. Cogliete l'occasione per sgranchirvi un po', guardare fuori dalla finestra, accarezzare il gatto e baciare il vostro partner (o viceversa).

Non finisce qui, anzi sì

In una miniguida come questa non c'è spazio per discutere le infinite varianti del concetto di backup partorite dalle menti troppo fervide degli informatici. La maggior parte di noi può vivere benissimo senza sapere la differenza fra un backup *incrementale* e un backup *differenziale*.

Quello che vi ho descritto qui è sufficiente per l'uso normale del computer e comunque è decisamente meglio del nulla totale che probabilmente avete avuto fin qui (ho indovinato, vero?).

Cosa fate ancora qui? Andate subito a fare un backup dei vostri dati!

Capitolo 10

Mettiamoci una pezza: aggiornamenti di Windows

Nessuno nasce perfetto, ma Windows è caduto da piccolo

Eccolo lì: l'avete appena comprato e spacchettato. È l'ultimo gioiello dell'informatica, con l'ultimissima versione di Windows. Il culmine di decenni di progresso tecnologico. E cosa fa, la prima volta che lo avviate? Reclama subito che lo dovete aggiornare. Ma come?

Mettetevi il cuore in pace: l'informatica è fatta così. Tutti i programmi (non solo Windows) contengono errori e falle che il controllo di qualità effettuato durante la loro realizzazione non riesce a snidare. Soltanto l'impatto con il mondo reale, e soprattutto con gli aggressori, consente di rilevare certe magagne e debolezze.

Di conseguenza, è prassi normale che i programmi subiscano una o più riparazioni post-vendita, un po' come avviene talvolta per le automobili. Per fortuna, invece di dover andare in officina, possiamo lasciare il computer attaccato a Internet e scaricare la riparazione, che verrà effettuata automaticamente dal computer, e tutti vivremo felici e contenti. Almeno in teoria.

Queste riparazioni, in gergo informatico, si chiamano *patch*, che si pronuncia come *pace* senza la E finale e letteralmente significa *"toppa"* o *"pezza"*. E in effetti è quello lo scopo: rattoppare i buchi dei programmi.

Senza le patch, sarebbe necessario attendere l'uscita nei negozi della versione successiva di Windows o del programma fallato per correggere il problema. Questo darebbe agli aggressori mesi e mesi di tempo per approfittare della vulnerabilità e richiederebbe costi enormi per la produzione e distribuzione di cataste di CD contenenti le nuove versioni.

Il sistema delle patch è insomma molto comodo. Così comodo che i produttori di programmi, purtroppo, ne approfittano. Invece di limitarsi a lasciare una o due correzioncine in sospeso, pur di rispettare le date di messa in vendita annunciate ne lasciano a badilate; tanto, dicono, c'è sempre la patch che aggiusta tutto. Si arriva così a estremi come i *sessantatremila* difetti piccoli e grandi lasciati in Windows 2000.[63]

Anche la concorrenza (Linux, Mac) ha le sue brave patch, ma si tratta di un fenomeno occasionale. Chi usa Windows, invece, ha a che fare con patch *mensili*, ciascuna delle quali raggruppa correzioni di varie falle. E non si tratta di semplici inestetismi: le falle turate dalle patch sono quasi sempre ad alto rischio, nel senso che consentono a un aggressore di devastare il computer della vittima o di prenderne il controllo.

Il guaio è che ogni tanto queste patch non funzionano a dovere: una volta installate, oltre a correggere la falla magari alterano il funzionamento del computer o introducono altre falle.[64] Una situazione da incubo.

In altre parole, le patch ricorrenti sono una delle peggiori scocciature che affliggono chi usa Windows. Ma senza le patch, Windows è un colabrodo esposto a una miriade di possibili infiltrazioni. Il povero utente si trova quindi fra l'incudine e il martello.

Fra l'altro, il semplice annuncio della disponibilità di una patch offre involontariamente una dritta agli aggressori, che si precipitano a studiare la falla che la patch corregge e a sfruttarla su chi non ha aggiornato il proprio Windows.

Insomma, non si scappa alla Regola 4 del Dodecalogo:

> ***Regola 4: Installate gli aggiornamenti (patch) di Microsoft***.

Ho paura del Grande Fratello

In teoria si può vivere sereni e felici anche senza le patch, ma soltanto se state dietro un buon firewall e non vi collegate a Internet, non *chattate* e non partecipate a circuiti di scambio di musica e film. Comprensibilmente, è uno scenario ormai sempre più raro.

Ma anche in un caso estremo del genere, vivere senza patch è un comportamento contrario a uno dei dogmi fondamentali della sicu-

rezza: mai avere un *single point of failure*, ossia un punto debole che, se compromesso, causa un disastro. Bisogna avere sempre più di un livello di protezione. Se per esempio il firewall viene violato o aggirato per qualsiasi ragione e non avete installato le patch, per voi si spalancano le porte dell'inferno informatico.

Molti utenti contrari alle patch temono l'effetto Grande Fratello (quello orwelliano, intendo), ossia che Microsoft le usi per intrufolarsi nel loro computer e fare lo spione. A parte il fatto che salvo casi rarissimi a Microsoft non potrebbe fregar di meno di quello che contiene il computer dell'utente medio, chi ha queste paranoie non ha forse considerato che se Microsoft o chi per essa volesse entrargli nel computer, potrebbe sfruttare proprio le vulnerabilità che le *patch* vogliono correggere.

E poi scusate, se non vi fidate di Microsoft, perché diavolo continuate a usare i suoi prodotti?

> *Un esempio lampante delle conseguenze di questa diffusa incoscienza è la devastazione causata ad agosto 2003 dal virus Blaster/Lovsan e ripetutasi a maggio 2004 con il virus Sasser.*
>
> *La patch che correggeva la falla sfruttata da quest'aggressore era già disponibile un mese prima che iniziasse a circolare il virus; nel caso di Blaster, persino il Dipartimento di Difesa statunitense aveva diramato avvisi invitando gli utenti a scaricare la patch. Ma milioni di utenti non l'avevano scaricata e installata e pertanto si sono infettati.*
>
> *Così imparano. Forse.*

Aggiornamenti automatici di Windows

In Windows è integrata una funzione, denominata ***Windows Update***, che a intervalli regolari chiede automaticamente a Microsoft se ci sono nuove correzioni e poi le scarica e installa.

Lo scopo di tutto quest'automatismo è alleviare il disagio dell'utente, ma è comunque **consigliabile disattivare l'aggiornamento automatico** e renderlo manuale, e quindi controllabile, per alcune ragioni fondamentali:

- come già accennato, ogni tanto le patch non funzionano o addirittura guastano Windows, per cui vanno installate soltanto quando si ha tempo di provvedere a un eventuale ripristino in caso di problemi, per esempio nel fine settimana;
- se lasciate le patch in mano agli automatismi, Windows può mettersi a scaricarle mentre state lavorando, rallentando la connessione a Internet e il funzionamento del computer;
- moltissimi utenti vedono comparire improvvisamente sullo schermo i vari fumetti che avvisano degli aggiornamenti (Figura 10.1), ma non li leggono perché hanno altro da fare in quel momento e li chiudono, con il risultato che le patch non vengono mai né scaricate né installate.

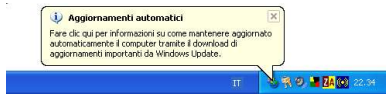

Figura 10.1

Riprendere il controllo è semplice. Se avete già aggiornato Windows XP con tutti gli aggiornamenti escluso il Service Pack 2, procedete come segue:

- *Start > Impostazioni > Pannello di controllo > Sistema.*
- Scegliete la scheda *Aggiornamenti automatici* e attivate *Disattiva gli aggiornamenti automatici.*

Se non avete ancora aggiornato Windows XP, la scheda *Aggiornamenti automatici* ha un aspetto diverso e occorre disattivare l'opzione *Mantieni aggiornato il computer*.

Fatto questo, non verrete più molestati dal fumetto che avvisa degli aggiornamenti, ma dovrete prendere l'abitudine di pianificare una visitina al sito Microsoft alla ricerca di patch almeno una volta la settimana, in un momento in cui avete tempo. **Se non l'avete, trovatelo.** Deve diventare una parte integrante della vostra routine di igiene informatica.

> *Talvolta l'installazione di un aggiornamento di Windows reimposta questo servizio e lo riattiva. Prendete l'abitudine di controllare che resti disattivato dopo ogni aggiornamento.*

A caccia di patch

Prima di installare una patch, è indispensabile **fare il backup di Windows**, creando come minimo un punto di ripristino, come descritto nel Capitolo 9; così se qualcosa va storto, potete tornare indietro.

Alcune installazioni di Windows creano automaticamente un punto di ripristino quando si installa una patch. Nel dubbio, comunque, è meglio creare un punto di ripristino in più che uno in meno.

Fatto il backup, collegatevi a Internet e scegliete Start > Windows Update. Viene lanciato Internet Explorer: per questa volta, dategli il permesso di uscire, perché si deve collegare al sito Microsoft.

Se compare una finestra intitolata *Avviso di protezione* che parla di *"installare ed eseguire Windows Update"*, come mostrato in Figura 10.2, **per questa volta** accettatela cliccando su *Sì*.

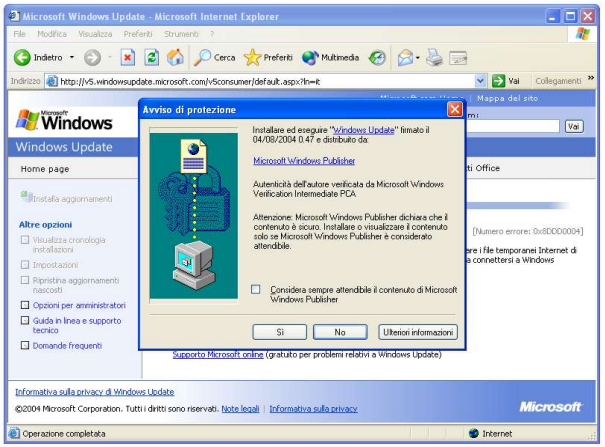

Figura 10.2

Questi "Avvisi di protezione" vanno trattati con estrema cautela. *In questo caso potete fidarvi, dato che l'avviso è comparso visitando esplicitamente il sito Microsoft.*

Se però compare visitando altri siti, oppure dopo aver cliccato su un indirizzo trovato in un e-mail, fate estrema attenzione prima di cliccare su Sì*: può trattarsi di un'e-*

sca per farvi installare un ***programma-spia*** *o un* ***"dialer"****, ossia un programma che vi collega a un numero telefonico a pagamento, come raccontato nel Capitolo 8.*

Nel dubbio, cliccate sempre su No.

La procedura di aggiornamento di Windows cambia spessissimo, per cui non stupitevi se quello che descrivo qui non coincide esattamente con quello che vedete sul vostro schermo. Ci sono comunque alcuni punti fondamentali che cambiano raramente:

- Se il sito Microsoft vi chiede di scaricare e installare un programma di gestione degli aggiornamenti più recente, accettate.
- Seguite le istruzioni che compaiono sullo schermo; se ci sono varie opzioni, scegliete quella etichettata *"consigliata*".
- Se il vostro firewall vi avvisa che ci sono programmi come *update.exe* che tentano di accedere a Internet durante l'aggiornamento di Windows, autorizzateli, ma non permanentemente.
- Se non avete mai aggiornato il vostro computer, cominciate perlomeno con gli aggiornamenti indicati da Microsoft come più urgenti o critici.
- Il primo aggiornamento è lungo: preparatevi a un'attesa notevole, dell'ordine delle decine di minuti, specialmente se siete collegati a Internet con una normale linea telefonica.
- Se vi viene chiesto di riavviare il computer, fatelo; poi ricollegatevi a Internet e lanciate di nuovo Windows Update per vedere se ci sono ulteriori aggiornamenti. Alcuni aggiornamenti, infatti, devono essere installati separatamente dagli altri e richiedono un riavvio prima di poter proseguire.
- È normale che Windows ogni tanto sembri apparentemente bloccato e che si senta il rumore del disco rigido che macina (Figura 10.3). Dategli un po' di corda prima di considerarlo impallato: controllate che non ci sia qualche finestra di dialogo in attesa di risposta, nascosta da altre finestre. Se Windows si impalla davvero, niente panico: riavviatelo e proseguite dal punto al quale eravate arrivati.

- Windows Update non funziona correttamente con *browser* (programmi di navigazione Web) alternativi: dovete usare per forza Internet Explorer.

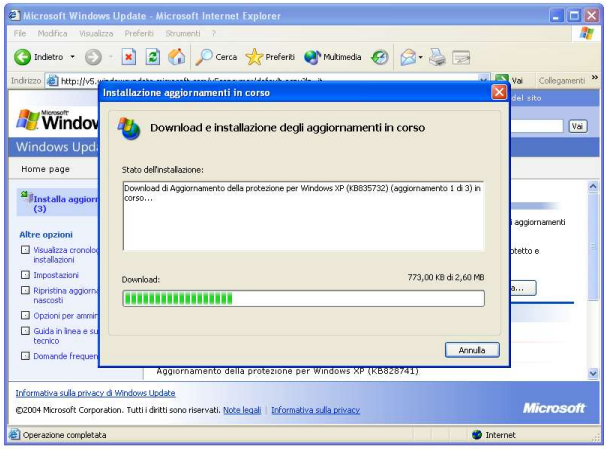

Figura 10.3

Patch non solo per Windows

Anche i programmi hanno le loro brave patch. In particolare le ha Microsoft Office, ed è molto importante installarle, perché anche Office è uno dei veicoli preferiti dagli aggressori, ed essendo ben integrato in Windows costituisce un percorso agevolato per raggiungere il cuore del sistema operativo.

Di conseguenza, è importante aggiornare anche Office con le relative patch, reperibili presso il sito *officeupdate.microsoft.com*.

Gli altri programmi, invece, raramente distribuiscono patch: offrono direttamente una versione nuova dell'intero programma. Anche in questo caso, aggiornare è importante, perché consente di chiudere le falle man mano che vengono scoperte.

Scaricare separatamente le patch

Una delle lamentele più frequenti riguardanti le patch è il tempo che ci vuole per scaricarle. Sono tante e sono *enormi*: altro che pezze, qui spesso si tratta di una coperta intera. Se non avete una

connessione veloce (ADSL o simili), lo scaricamento delle patch dura ore; e se per qualsiasi ragione dovete reinstallare Windows, dovete scaricare *di nuovo* tutte le patch. Non so voi, ma io ho cose migliori da fare nella vita.

Per fortuna c'è un rimedio: le patch sono scaricabili e salvabili su disco anche senza installarle. Potete chiedere a un amico dotato di connessione veloce di scaricarvele e scriverle su un CD, che poi userete per aggiornare il vostro Windows tutte le volte che volete (o dovete).

Chiaramente con questo metodo si perde gran parte della gestione automatica delle patch offerta da Windows Update, ma è comunque un'alternativa tutt'altro che trascurabile, specialmente per le patch più grandi, denominate *Service Pack*.

Se scaricate le patch senza usare Windows Update, scoprirete che sono dei semplici file di programmi (come evidenziato dalla loro estensione *exe*). Una volta che ve le siete procurate, non dovete far altro che lanciarle come se fossero comuni programmi.

Interessante, ma dove ci si procura queste patch scaricabili? Ci sono due fonti fondamentali:

- i CD allegati alle riviste d'informatica;
- le apposite sezioni del sito Microsoft.

> ***Le patch non vengono mai distribuite come allegati a e-mail**. Se ricevete un e-mail che vi chiede di installare la patch allegata, **non fatelo**, neppure se il messaggio sembra provenire da Microsoft: è un tentativo di intrusione o di infezione.*

Il catalogo delle pezze

Per scaricare le patch dal sito Microsoft senza installarle, conservandole per un uso successivo, procedete come segue:

- Avviate come prima Windows Update, ma stavolta cliccate su *Opzioni per amministratori* nella pagina del sito Microsoft che compare. Da qui, cliccate sul *Catalogo di Windows Update* (Figura 10.4) e scegliete *Trova aggiornamenti per i sistemi operativi Microsoft*.

- Scegliete il vostro sistema operativo nel menu: otterrete un elenco di risultati suddivisi in categorie.
- Cliccate su una categoria (per esempio quella degli aggiornamenti consigliati) e cliccate su *Aggiungi* in ciascuna patch desiderata, scegliendo le versioni corrispondenti alla lingua del vostro Windows. Ripetete per ciascuna categoria.
- Le patch selezionate finiscono nel cosiddetto *Raccoglitore download*: cliccate sul pulsante omonimo e poi su *Sfoglia* per scegliere la cartella del vostro disco rigido dove verranno salvate le patch che avete scelto.

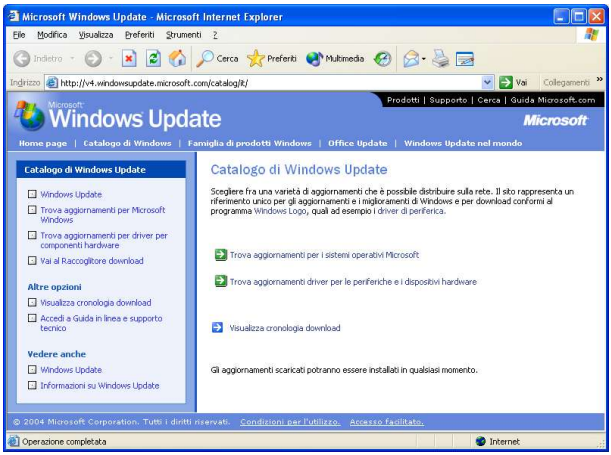

Figura 10.4

- Una volta fatta la scelta, cliccate su *Download*.
- Durante lo scaricamento vi verrà probabilmente chiesto di accettare alcune licenze.

Al termine di questa procedura, nella cartella che avete scelto trovate le varie patch scaricate. Quando volete, eseguitele con un doppio clic per installarle e fatene una copia su un CD, in modo da poterle riusare in caso di reinstallazione da capo di Windows.

L'Area Download di Microsoft

Un altro modo per salvare le patch senza installarle e per conservarle per usarle in seguito o su altri computer è accedere con In-

ternet Explorer all'*Area Download* del sito Microsoft (*www.microsoft.com/downloads/search.aspx?langid=12&displaylang=it*). Da qui potete scaricare e salvare su disco praticamente tutte le patch e i Service Pack disponibili.

Per sapere esattamente quali patch servono per un specifico computer, potete usare il Windows Update di quel computer per visitare il sito Microsoft come se doveste scaricarne gli aggiornamenti ma limitarvi invece a prendere nota dei loro codici di riferimento. Armati di questi codici, andate all'Area Download e li immettete nell'apposita casella di questa pagina del sito Microsoft per scaricare la patch corrispondente.

Anche in questo caso, una volta salvate le patch, potete installarle semplicemente eseguendole, come se fossero normali programmi. Questa è la soluzione più comoda se dovete chiedere a qualcuno di scaricarle per voi, per esempio perché non avete una connessione veloce.

L'unico svantaggio di questo metodo è che richiede un po' di operazioni manuali: il metodo "ortodosso" di usare Windows Update, invece, decide tutto da solo. A voi la scelta.

Verificare che una patch funzioni

Purtroppo non c'è una tecnica standard per verificare l'efficacia delle patch di Windows: il metodo da usare varia a seconda del problema risolto dalla specifica patch. Spesso, oltretutto, Microsoft non spiega esattamente qual è il problema risolto dalla patch, per non dare troppe imbeccate ai vandali, e quindi è impossibile creare le specifiche condizioni in cui la patch deve agire.

Ci sono comunque vari siti dedicati alla sicurezza che offrono test per singole patch: per esempio, Grc.com ne offre uno per la cosiddetta *"patch DCOM"* (*grc.com/dcom/*), ma le patch sono troppo numerose per poter elencare qui ogni singolo test disponibile.

Se volete fare questo genere di verifica, vi conviene frequentare i siti e i notiziari su Internet dedicati alla sicurezza, che spesso segnalano sia le nuove patch, sia la maniera di testarle.

Verificare il funzionamento di una patch non è un futile esercizio di paranoia. Innanzitutto, constatare di persona che una falla che prima c'era ora non c'è più è un forte incentivo ad adottare le patch,

che troppi utenti snobbano anche perché non ne percepiscono l'efficacia. In secondo luogo, non sempre le patch funzionano come dichiarato,[65] e talvolta non funzionano del tutto, per cui è meglio comunque dare una controllata.

La madre di tutte le patch: il Service Pack 2

Il Service Pack 2 è un aggiornamento talmente massiccio e importante che è necessario parlarne separatamente. Non solo contiene tutte le patch di Windows XP pubblicate da Microsoft fino a settembre 2004, ma altera profondamente il modo di funzionare di Windows e lo rende un po' meno insicuro. Purtroppo è anche gigantesco: a seconda dei casi, può variare da 70 a 270 megabyte.

Microsoft ha predisposto le cose in modo che sia scaricabile anche a puntate, per così dire, ma se non avete una connessione veloce, vi ci vorranno ore e ore. Così, in via del tutto eccezionale, Microsoft ha deciso di offrire un CD gratuito contenente il Service Pack 2 a chiunque ne faccia richiesta. Le istruzioni per riceverlo sono sul sito Microsoft.[66]

> *Il Service Pack 2 non è incluso nei computer Windows XP risalenti a prima di settembre 2004. I computer nuovi in vendita dopo quella data, invece, dovrebbero già includerlo direttamente.*[67]
>
> *Per sapere se il vostro Windows XP include già il Service Pack 2, andate in Esplora risorse, scegliete la Guida e la voce* Informazioni su Windows.

L'importanza dei preliminari

Come per qualsiasi patch, anche per il Service Pack 2 vale la raccomandazione fondamentale: **fate un backup prima di installarlo.** Il Service Pack 2 rassetta radicalmente le interiora di Windows XP ancor più di una normale patch, per cui **è facile che dopo l'installazione qualcosa non funzioni** (compresa, purtroppo, l'opzione di disinstallare il Service Pack 2)**.** In tal caso, soltanto il backup vi salverà.

A parte questo, nel caso del Service Pack 2 ci sono alcune incombenze supplementari da non sottovalutare e da completare prima di installare quest'aggiornamento:

- Il Service Pack 2 causa problemi soprattutto se viene installato su un Windows "sporco", ossia contenente virus, dialer e spyware. Pertanto, prima di cominciare, eseguite una pulizia accurata con un antivirus e un antispyware aggiornati.
- **Liberate spazio** sul disco rigido. *Molto* spazio. La raccomandazione ufficiale di Microsoft è di lasciare liberi **almeno 1800 megabyte**.
- Se potete, **aggiornate i vostri programmi** alla loro versione più recente.[68] Questa raccomandazione vale anche per l'antivirus e il firewall. Il Service Pack 2 può dare problemi alle vecchie versioni dei programmi, se non sono state progettate in base ai nuovi criteri di sicurezza Microsoft. Se non esiste una versione aggiornata di un programma che vi serve, non vi resta che sperare in bene.

I postumi di un'installazione del Service Pack 2 sono talvolta pesanti. Molti utenti lamentano addirittura malfunzionamenti e disagi: Microsoft ha pubblicato un elenco di oltre duecento programmi che non funzionano del tutto, oppure funzionano in modo anomalo, dopo l'installazione del Service Pack 2 presso *support.microsoft.com/default.aspx?kbid=884130*. L'elenco include programmi molto diffusi, come Unreal Tournament, McAfee VirusScan 7, Adobe PageMaker 7 e persino alcune versioni di Microsoft Office.

Inoltre il Service Pack 2 non pone fine a tutti i problemi di sicurezza. Ci saranno sicuramente ulteriori patch per correggere le falle scoperte dopo la sua pubblicazione, per cui non adagiatevi pensando che dopo il Service Pack 2 non ci saranno più aggiornamenti. La fatica, insomma, non finisce qui.

Cosa cambia con il Service Pack 2

In aggiunta alle novità descritte negli altri capitoli, il Service Pack 2 ha anche effetto sul sistema degli aggiornamenti. Il *Centro Sicurezza PC,* il nuovo servizio di aggiornamento che trovate in Windows XP dopo aver installato il Service Pack 2, non solo rende più snella l'installazione delle patch, ma consente anche di rimuoverle singolarmente (tramite *Start* > *Pannello di controllo* > *Installazione*

applicazioni > *Cambia/Rimuovi programmi*) se vi accorgete che causano problemi.

Le opzioni di automazione degli aggiornamenti sono state riordinate e descritte più chiaramente: sono in *Start* > *Pannello di controllo* > *Aggiornamenti automatici* e ora comprendono quattro possibilità di scelta:

- scaricamento e installazione completamente automatica (patch a sorpresa, insomma);
- scaricamento automatico e installazione manuale;
- semplice avviso di disponibilità, senza scaricamento e senza installazione;
- disattivazione completa.

Protezione antivirus integrata: DEP

Una delle novità più tecniche e meno vistose del Service Pack 2 è il cosiddetto DEP (*Data Execution Prevention*). È una funzione di sicurezza che serve a impedire che virus o programmi difettosi possano invadere aree di memoria che non spettano loro e quindi far disastri. Se funziona, è un ammazzavirus di prima categoria.

Al momento, tuttavia, molti processori per PC non incorporano ancora direttamente questa funzione: in tal caso, Windows la emula.

Non sbadigliate! La faccenda è importante perché questa emulazione comporta un aggravio di lavoro per il processore, che può portare a un rallentamento anche vistoso di Windows dopo aver installato il Service Pack 2.

Se notate che Windows sembra nuotare nella melassa dopo il Service Pack 2 o addirittura avete programmi che non funzionano del tutto (per esempio programmi per vedere i filmati DivX), provate a disattivare il DEP: è accessibile nel Pannello di Controllo, sotto *Sistema*. Scegliete la scheda *Avanzate* e cliccate su *Impostazioni* nella prima sezione in alto di questa scheda: troverete una scheda intitolata *Protezione esecuzione programmi*.

Normalmente, il DEP viene attivato soltanto a protezione dei servizi e programmi essenziali di Windows, ma potrebbe anche essere stato attivato per tutti i programmi, causando un rallentamento. Se è così, provate ad attivarlo soltanto per i programmi e servizi es-

senziali, in modo da ridurre il carico di lavoro svolto dall'emulazione software.

Se neppure questo risolve il rallentamento, esiste anche un'opzione di disattivazione completa, che però richiede qualche piccola acrobazia: in pratica, bisogna modificare a mano il file di sistema *boot.ini*, sostituendo con *AlwaysOff* il valore indicato dopo il segno di uguale nel parametro */NoExecute.* Non sentitevi in imbarazzo a chiedere l'aiuto di uno smanettone: sono modifiche piuttosto delicate.

Naturalmente queste modifiche comportano la rinuncia parziale o totale alla protezione antivirus offerta dal DEP; pertanto valutatele con attenzione.

Novità dietro le quinte

Le modifiche introdotte dal Service Pack 2 sono troppo numerose per poterle elencare qui. Vale la pena di segnalarne comunque qualcuna:

- il supporto per i dispositivi senza fili *Bluetooth* (telefonini, computer palmari, accessori per PC), che prima era necessario installare separatamente;
- la disabilitazione del servizio Messenger, responsabile di una particolare forma di pubblicità indesiderata descritta nel Capitolo 4 (il *Messenger spam*)
- l'aggiornamento automatico di Windows Media Player alla versione 9 per turarne alcune falle di sicurezza e cambiare la gestione dei diritti digitali (sistemi anticopia), anche se è comunque già disponibile la versione 10, ulteriormente aggiornata;
- il rafforzamento della sicurezza di Windows Messenger, un popolare programma per chattare;
- un nuovo sistema di gestione che semplifica e irrobustisce l'uso delle connessioni senza fili, comprese quelle che sempre più spesso sono disponibili nei luoghi pubblici (*hotspot*).

Nel loro complesso, queste modifiche sono effettivamente molto utili per rendere Windows XP un po' meno amico dei pirati informatici. Vale la pena di affrontare qualche tribolazione durante l'installazione del Service Pack 2 pur di acquisirle.

Capitolo 11

Web sicuro: imbavagliare Internet Explorer

C'era una volta il Web

Molti utenti che si avvicinano a Internet per la prima volta si chiedono cosa ci trovino di così bello gli altri utenti della Rete. Chi gliel'o fa fare di entrare in un ambiente dove basta visitare una pagina sbagliata per infettarsi o far collassare il computer e gli aggressori sono sempre pronti a far schizzare sullo schermo finestre piene di pornografia e a bombardarci di virus? Sembra divertente come passeggiare per un quartiere malfamato con un Rolex al polso e i diamanti al collo.

In realtà, chi frequenta la Rete da tempo sa che Internet non è sempre stata così infestata. Quando nacque il Web, nell'informaticamente lontanissimo 1991,[69] non era possibile infettare un computer semplicemente visualizzando una pagina Web o ricevendo un e-mail. La pornografia in Rete c'era già, ma non saltava fuori all'improvviso se non la si andava a cercare. Navigare era un piacere sicuro come sfogliare un libro.

Le cose cominciarono a cambiare quando Microsoft incluse in Windows un *browser*, ossia un programma per la navigazione nei siti Web, chiamato *Internet Explorer*. Prima, infatti, Windows non ce l'aveva: bisognava scaricarlo a parte. Si poteva così scegliere facilmente fra vari tipi di browser concorrenti: il leader incontrastato del mercato, all'epoca, si chiamava *Netscape*, discendente del primissimo browser grafico denominato *Mosaic*. Ma trovandosi Internet Explorer preinstallato, moltissimi utenti non cercarono più alternative, anche se la concorrenza era tecnicamente superiore.

Purtroppo Microsoft fece alcuni errori fondamentali. Per esempio, per ragioni principalmente commerciali (ossia per "togliere l'ossigeno" alla concorrenza di Netscape, come indicato dagli atti del processo antitrust USA), fece diventare Internet Explorer una parte inscindibile di Windows. Questa scelta fu (ed è tuttora) un disa-

stro in termini di sicurezza: un difetto del browser diventa infatti un difetto del sistema operativo, permettendo l'accesso alle parti più vitali del computer. Un browser installato a parte, invece, "siede sopra" Windows, senza integrarvisi, per cui se il browser ha delle falle, Windows rimane in piedi.

Il secondo errore fu decidere di rendere Internet più bella, sgargiante e vivace, ma soprattutto *facile*, creando nuove versioni di Internet Explorer che permettevano alle pagine Web di contenere animazioni, immagini, effetti interattivi (per esempio i totali che si calcolano da soli nei negozi online) e in particolare programmi che si eseguono e installano da soli senza affaticare l'utente.

Ovviamente gli aggressori e i commercianti senza scrupoli approfittarono subito di queste novità, creando appunto programmi autoinstallanti ostili, in grado di pilotare la vittima verso i loro siti Web e verso le loro linee telefoniche a tariffa maggiorata o altri servizi truffaldini. E così si arrivò al letamaio telematico di oggi.

Per fortuna esiste ancora un modo molto semplice per ritornare all'Internet sicura dei vecchi tempi: sbarazzarsi di Internet Explorer. Ecco il motivo della Regola 6 del Dodecalogo:

> ***Regola 6: Non usate Internet Explorer e Outlook Express.*** *Sostituiteli con prodotti alternativi più sicuri.*

In questo capitolo vi mostrerò come potete procurarvi e usare browser alternativi che non solo sono più sicuri, ma sono anche gratuiti e più pratici e versatili del prodotto Microsoft.

Cosa c'entra Outlook Express?

Probabilmente vi state chiedendo perché la Regola 6 include anche Outlook Express. Cosa c'entra un programma per la posta con un programma per navigare nel Web?

Semplice: Outlook Express utilizza pezzi di Internet Explorer per alcune funzioni (per esempio la visualizzazione degli elementi grafici dei messaggi). Se c'è una falla in Internet Explorer, ne risente quindi anche Outlook Express e viceversa. Quindi per curare il problema dovete sbarazzarvi di entrambi.

> ***Ma come, ma se* tutti *usano Internet Explorer e Outlook Express!*** *Certo, e i risultati si vedono. Le infezioni*

di massa sono dovute proprio al fatto che tantissimi utenti adoperano questi due programmi insicuri.

*Entrambi, non a caso, sono nella top ten delle maggiori vulnerabilità di Windows pubblicate dal Sans Institute, una delle più rinomate fonti di informazioni sulla sicurezza informatica (*www.sans.org/top20/*).*

La vera grana è che sbarazzarsi completamente di questi programmi, e in particolare di Internet Explorer, non è permesso. **In Windows XP non si può disinstallare completamente Internet Explorer**, proprio perché Microsoft l'ha intrecciato inestricabilmente con Windows.

Siete obbligati a tenere Internet Explorer anche se non lo volete e anche se non lo usate: è come se la Gillette vi obbligasse a comperare la sua schiuma da barba ogni volta che comperate le lamette, anche se quella schiuma vi rovina la pelle. Esistono programmi come *IE Eradicator* e *XPLite* (*www.litepc.com*) che eliminano molti dei file di Internet Explorer, ma non tutti.

Si può comunque ottenere un risultato ragionevole, dal punto di vista della sicurezza, semplicemente **non usando Internet Explorer.** Se non lo invocate, se ne starà lì senza fare danni. Non troppi, perlomeno.

La prima cosa da fare, insomma, è **procurarsi un browser sostitutivo**; nel prossimo capitolo vi mostrerò come sostituire anche Outlook Express (o perlomeno irrobustirlo un po', se non riuscite ad abbandonarlo).

La seconda cosa che occorre fare è **irrobustire comunque Internet Explorer**. Ci sono infatti alcuni siti che incoscientemente funzionano soltanto con questo browser, per cui ogni tanto può rivelarsi necessario usarlo (il bello è che molti di questi siti appartengono a banche e impongono Internet Explorer "per motivi di sicurezza"). In tal caso, bisogna fare in modo di usarlo esponendosi il meno possibile a rischi di aggressione.

I criteri fondamentali che vi conviene seguire per una navigazione meno insicura nel Web sono insomma questi:

- **usate un browser alternativo per la navigazione normale;**

- **usate Internet Explorer soltanto se vi imbattete in uno dei (pochi) siti che funzionano esclusivamente con Internet Explorer;**
- **in ogni caso, usate Internet Explorer soltanto su siti affidabili** (istituzioni, banche e simili).

> *Se non siete del tutto convinti della necessità di abbandonare Internet Explorer, vi invito a usarlo per visitare i siti dimostrativi elencati verso la fine di questo capitolo, nel paragrafo* Come collaudare il browser.
>
> *Scoprirete quant'è facile far leva su Internet Explorer per fare disastri. Chiedete a un amico che usa un altro browser di fare questi stessi test e vi accorgerete della differenza.*
>
> *Certo, nessun browser è totalmente sicuro, ma Internet Explorer è di gran lunga uno dei meno sicuri, anche perché la sua larghissima diffusione lo rende un bersaglio molto appetibile.*

Procurarsi un browser alternativo

Fra i browser alternativi a Internet Explorer c'è soltanto l'imbarazzo della scelta. Ecco alcuni dei più diffusi e collaudati:

- **Firefox**
  (*www.mozilla.org*, disponibile anche in italiano presso *www.mozillaitalia.org*)
  Completamente gratuito, browser puro e senza accessori, estremamente leggero e veloce; include la gestione dei *feed RSS*, un modo molto pratico di sintetizzare le informazioni provenienti da tanti siti Web.
- **Mozilla**
  (*www.mozilla.org*, disponibile anche in italiano presso *www.mozillaitalia.org*)
  Completamente gratuito, include anche funzioni per la creazione di pagine Web, per la gestione della posta, per il chat IRC e per i newsgroup.
- **Opera**
  (*www.opera.com*, disponibile anche in italiano)

Disponibile in versione gratuita sostenuta da piccole immagini pubblicitarie o in versione a pagamento senza pubblicità; include gestione della posta e delle chat IRC, feed RSS.

- **Netscape**
  (*www.netscape.com*, non disponibile in italiano)
  Completamente gratuito, include funzioni per la creazione di pagine Web e per la gestione di chat (AOL), ICQ e posta.

Fra l'altro, questi browser alternativi non sono soltanto meno insicuri: sono anche oggetto di minori attenzioni da parte degli aggressori informatici, perché sono meno diffusi di Internet Explorer; per cui quando hanno delle falle, è raro che vengano sfruttate in modo ostile prima che vengano corrette.

Come ciliegina sulla torta, i browser alternativi sono anche tecnicamente più evoluti:

- **bloccano le pubblicità:** molti siti fanno comparire fastidiosissima finestre pubblicitarie sopra la pagina Web che volete leggere: si chiamano *"popup"*. Questi browser possono bloccarle. Internet Explorer è in grado di farlo soltanto se lo aggiornate con il Service Pack 2.
- **gestiscono pagine multiple tramite linguette o "schede" *(tabbed browsing*)*:*** invece di avere tante finestre del browser, una per ciascuna pagina che state visitando, come fa Internet Explorer, potete avere una singola finestra che le gestisce tutte e permette di passare da una pagina Web all'altra cliccando sulle loro linguette, come se le pagine fossero fogli di uno schedario (Figura 11.1). È comodissimo, ma molto più difficile da descrivere che da provare: fatelo, non tornerete più indietro.
- **capiscono i gesti del mouse:** invece di dover cliccare sui pulsanti di navigazione, potete dire a questi browser di riconoscere un certo movimento del mouse. Per esempio, se tenete premuto il pulsante destro del mouse mentre muovete il mouse verso sinistra, Opera torna alla pagina precedente.
- **salvano le navigazioni in corso:** potete chiedere a questi browser di ricordarsi le pagine Web che state consultando, così la prossima volta che avviate il computer potete ricominciare da dove eravate rimasti, senza dover frugare nella Cronologia come si fa con Internet Explorer.

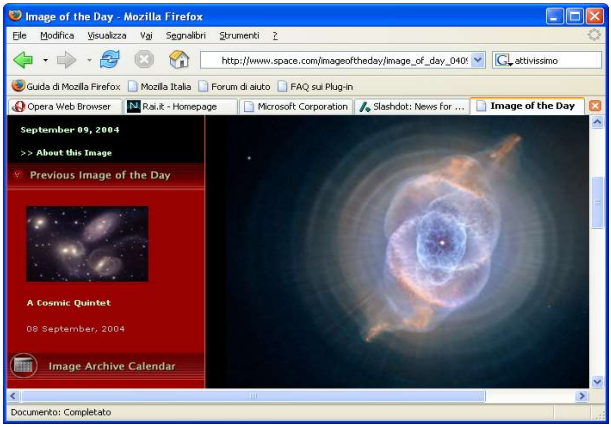

Figura 11.1

- **offrono ricerche velocissime:** con Internet Explorer, per cercare qualcosa dovete andare a *www.google.it* (o al vostro motore di ricerca preferito), attendere che venga visualizzata la pagina iniziale di Google e poi immettere l'oggetto della vostra ricerca. Con i browser alternativi, vi basta immettere l'oggetto della ricerca nell'apposita casella della finestra del browser, accanto alla casella dove si digitano gli indirizzi dei siti (Figura 11.2) per ottenere direttamente i risultati forniti da Google o dal motore di ricerca che preferite.

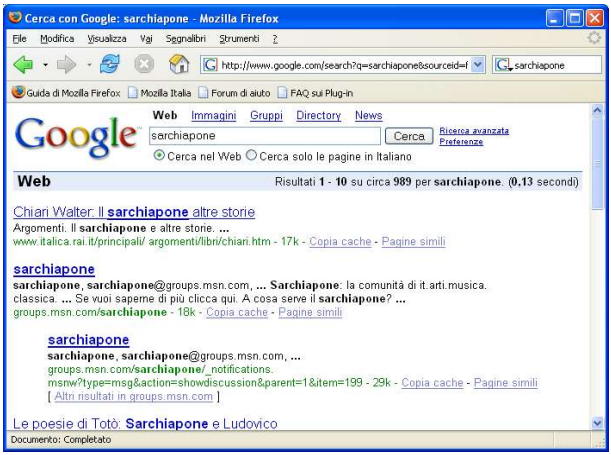

Figura 11.2

*Esistono alcuni programmi, come SlimBrowser (*www.flashpeak.com*), che in realtà non sono browser autonomi; sfruttano parti di Internet Explorer aggiungendovi alcune di queste funzioni molto utili. Tuttavia non risolvono il problema di fondo: essendo basati su Internet Explorer, ne ereditano le falle. Lasciate dunque perdere queste soluzioni a metà e adottate direttamente un browser alternativo.*

Cambiare browser si può, anzi si deve

Rinunciare a Internet Explorer non è un'impresa particolarmente impegnativa. In genere richiede tre semplici passi:

- scaricare e installare un browser alternativo;
- importare i *Preferiti* (l'agenda degli indirizzi dei siti che vi interessano), le opzioni, i segnalibri, la cronologia e le password di Internet Explorer;
- impostare il nuovo browser come *browser predefinito*.

Tutto questo avviene direttamente durante l'installazione: a un certo punto vi viene chiesto (in italiano) se volete importare i Preferiti e se volete che il nuovo browser diventi quello principale (o *predefinito* o *di default*), ossia quello che verrà lanciato quando cliccate su un indirizzo Web in un e-mail o in un documento.

A questo punto potete già cominciare a navigare più tranquilli. Vedrete molta meno pubblicità e potrete girare la Rete in lungo e in largo senza l'angoscia di trovarvi il computer infetto o paralizzato. Vi conviene comunque non abusare di questa maggiore sicurezza, perché anche i browser alternativi ogni tanto rivelano qualche falla. Non pensate insomma di essere diventati invincibili: siete semplicemente meno indifesi di prima, ed è già tanto, credetemi.

C'è inoltre ancora un po' di lavoro da fare prima di raggiungere il massimo della sicurezza: addomesticare Internet Explorer, in modo che si comporti bene quando (raramente) vi serve proprio usarlo, e imparare alcune regole di navigazione sicura per proteggersi da bufale, burle e truffe.

Blindare Internet Explorer

Irrobustire Internet Explorer è purtroppo necessario anche se non lo usate: essendo integrato strettamente in Windows, le sue falle talvolta si ripercuotono sull'intero sistema anche quando non lo adoperate per navigare. Alcuni suoi componenti, infatti, sono sempre in uso, anche quando usate un browser alternativo.[70]

Inoltre ci sono, come dicevo, alcuni siti che si ostinano a non rispettare gli standard ufficiali di Internet e sono compatibili soltanto con il browser di mamma Microsoft (ebbene sì, **Internet Explorer non rispetta gli standard**). Di conseguenza, ogni tanto occorre adoperare Internet Explorer, ed è importante che quando lo usate non corriate rischi inutili.

Ecco una rassegna di trucchetti per minimizzare i pericoli.[71]

> ***Non prendete questi "irrobustimenti" come una scusa per continuare a usare Internet Explorer*** *per tutte le vostre navigazioni: sono sufficienti soltanto per un uso occasionale del browser Microsoft su siti che presumete siano affidabili.*
>
> *Rimane valida la raccomandazione di usare un browser alternativo* sempre e comunque*, salvo necessità di singoli siti fidati.*

Svecchiate Internet Explorer!

La primissima cosa da fare per rendere Internet Explorer meno vulnerabile è usare il solito Windows Update per scaricarne la versione più aggiornata, che è quella nella quale è stato turato il maggior numero di falle conosciute.

È inutile cercare di addomesticare un Internet Explorer vecchio: resterebbero comunque troppe vulnerabilità ben note agli aggressori. Gli aggiornamenti apportati dal Service Pack 2, in particolare, sono estremamente importanti.

Tu di qui esci quando lo dico io

La seconda cosa da fare è **impostare il firewall in modo che Internet Explorer non sia abilitato automaticamente a uscire**, ma debba chiedervi ogni volta il permesso, e autorizzare invece per-

manentemente il vostro browser alternativo. Qualsiasi firewall decente è in grado di farlo.

In questo modo, se Internet Explorer viene avviato per qualsiasi ragione (da un virus o da una pagina Web o da un e-mail), verrete avvisati e potrete bloccarlo, mentre la navigazione più sicura del browser alternativo verrà agevolata.

Pagina iniziale inutile

Quando lo avviate, Internet Explorer va subito a cercare il sito Web di Microsoft. È una perdita di tempo, dato che di solito lanciate Internet Explorer per andare a visitare il sito che interessa a voi, non quello che a Microsoft interessa promuovere.

Per non caricare la pagina Microsoft all'avvio di Internet Explorer:

- lanciate Internet Explorer e scegliete Strumenti > Opzioni Internet;
- cliccate sulla scheda *Generale* e poi sul pulsante *Pagina vuota*;
- cliccate su OK.

Chiudendo e riavviando Internet Explorer, noterete che non carica più la pagina di Microsoft.

Rassegnati, non sei più il mio predefinito

Quando scegliete il browser alternativo come predefinito, Internet Explorer si offende: vi chiede insistentemente se volete che torni a essere lui il predefinito.

Per farlo smettere, quando lo avviate, rispondete alla richiesta disattivando la casella *Esegui sempre il controllo all'avvio di Internet Explorer* e poi cliccando su *No.*

In alternativa, scegliete *Strumenti* > *Opzioni Internet* e la scheda *Programmi* e disattivate la casella *Verifica che Internet Explorer sia il browser predefinito*.

Opzioni avanzate

In Internet Explorer, scegliete *Strumenti* > *Opzioni Internet*, cliccate sulla scheda Avanzate e controllate che le seguenti opzioni siano impostate correttamente (se non lo sono, cambiatele):

- *Abilita estensioni dei browser di terze parti:* disattivata, per impedire a molti programmi-spia e accessori per Internet Explorer più o meno impiccioni di autoinstallarsi.
- *Abilita installazione su richiesta (altro)* e *Abilita installazione su richiesta (Internet Explorer)*: disattivate, così un sito non può indurre Internet Explorer a chiedervi di installare software aggiuntivo per visualizzare le pagine Web. Questo rende più sicuro Internet Explorer, ma può causare problemi di visualizzazione con pagine che richiedono la presenza di questi programmi aggiuntivi sul vostro computer.
- *Attiva Profile Assistant*: disattivata. In questo modo, se avete memorizzato dati personali nel Profile Assistant, i siti troppo curiosi non possono prelevarli automaticamente.
- *Avvisa in caso di certificati di siti non validi:* attivata. Molti siti Web usano dei cosiddetti *certificati digitali* per autenticarsi. Purtroppo Internet Explorer normalmente non verifica se questi certificati sono stati revocati, per esempio perché qualche malintenzionato se ne è impadronito. Diventa così facile creare un sito ostile che è apparentemente "garantito" da un certificato in realtà revocato.
- *Avvisa se la sottoscrizione delle schede viene reindirizzata:* attivata. Se compiliamo un modulo contenuto in una pagina Web e i dati immessi vanno a un sito diverso da quello che contiene il modulo (tipico trucco degli spioni), scatta un avviso.
- *Verifica revoca dei certificati del server* e *Verifica revoca dei certificati dell'autore*: attivate. Si tratta ancora di certificati digitali di autenticazione, che è meglio controllare sempre.

Fidarsi è bene, non fidarsi è meglio: aree di protezione

Internet Explorer gestisce le pagine Web in modo diverso in base all'*area* dalla quale provengono: si fida molto delle pagine custodite nel vostro computer e nei computer della rete locale (se ne avete una) e poco di quelle che arrivano da Internet.

Questa gestione è controllata tramite una scheda intitolata *Protezione*, che trovate in Internet Explorer sotto *Strumenti* > *Opzioni Internet*. Se cliccate sull'icona *Internet*, noterete che la protezione

predefinita per le pagine che provengono dalla Rete è *Media*; per le pagine della rete locale (*Intranet locale*) è addirittura *Medio-bassa*.

In realtà, oltre all'area *Internet* e a quella *Intranet locale*, ce n'è un'altra, *Risorse del Computer,* che riguarda i dati provenienti dal vostro computer, ma per motivi insondabili non viene visualizzata. Come dicevo, Windows fa i dispetti.

> *L'area Risorse del Computer può essere rivelata soltanto con un intervento molto delicato,*[72] *descritto nel supplemento* Per veri smanettoni *di questo libro, presso* www.attivissimo.net *e da affidare a mani esperte; è importante rivelarla per poterla impostare, perché Windows si fida* ciecamente *di quello che proviene (o sembra provenire) da quest'area.*

Tutto questo è *male*, perché gli aggressori conoscono un sacco di trucchetti per far credere a Internet Explorer che le loro pagine provengano dalle aree fidate *Intranet locale* e *Risorse del Computer* e indurre quindi il browser Microsoft ad abbassare le difese ed eseguire le istruzioni nascoste in quelle pagine, per esempio per devastarvi il PC o più probabilmente infettarlo silenziosamente.[73]

Conviene quindi assegnare a *tutte* le aree la stessa protezione, ossia *Media* o meglio ancora *Alta* (cliccando su *Livello predefinito* per far comparire il selettore di livello), in modo che Internet Explorer rimanga sospettoso anche quando crede erroneamente di avere a che fare con pagine locali.

Ma cosa significano di preciso queste etichette *Alta, Media, Medio-bassa* e *Bassa*? La spiegazione ha a che fare con la Regola 7 del Dodecalogo, valida non soltanto per Internet Explorer, ma **per tutti i browser**:

> ***Regola 7: Tenete disattivati ActiveX, Javascript e Visual Basic Scripting.*** *Riattivateli soltanto quando visitate siti di indubbia reputazione.*

Questi nomi vi sono forse poco familiari: semplificando, identificano linguaggi di programmazione che consentono di annidare veri e propri microprogrammi (detti anche *script*) all'interno di e-mail e pagine Web.

Così le pagine di Internet diventano più belle, colorate e interattive: ma gli aggressori informatici sanno manipolare questi linguaggi per creare microprogrammi ostili.[74]

> *Attenti a non confondere* Javascript *con* Java*. Sono due linguaggi profondamente diversi, il cui unico legame sta nel nome un po' ingannevole. Javascript è facilmente sfruttabile dagli aggressori: Java lo è soltanto con estrema difficoltà ed è purtroppo in via di estinzione sui PC Windows; per questo non è citato nella Regola 7.*[75]

La principale differenza fra i vari livelli di protezione di Internet Explorer è il modo in cui vengono gestiti questi linguaggi: se la protezione è *Alta*, non vengono eseguiti; se la protezione è *Media,* vengono eseguiti automaticamente, in alcuni casi chiedendo conferma; se la protezione è *Medio-bassa* o *Bassa*, viene eseguito tutto senza alcuna conferma o esitazione e tanto vale dipingersi addosso un bersaglio. È per questo che è opportuno impostare la protezione ad *Alta*.

Il guaio è che così facendo, molti siti che sfruttano questi linguaggi per ottenere effetti interattivi o grafici utili e accattivanti non funzionano: succede per esempio con il sito Windows Update di Microsoft e con quelli di alcune banche, servizi e negozi online. La protezione *Alta* blocca anche lo scaricamento *volontario* di file tramite Internet Explorer.

In casi come questi, **se vi fidate del sito** (ossia se si tratta della vostra banca, non certo di un sito che "regala" aiutini per la maturità o calendari di celebrità svestite), potete abbassare leggermente la guardia e portare il livello a *Media*.

> *Se avete reso visibile l'area Risorse del computer, per impostarla ad* Alta *cliccate sull'icona e poi sul pulsante* Livello personalizzato*, scegliete* Alta *e cliccate su* Reimposta*.*
>
> *Tenete presente che in alcune circostanze Windows usa questi linguaggi anche per mostrarvi pagine informative sullo stato del vostro computer. Impostando l'area Risorse del computer ad* Alta*, Windows non potrà visualizzarle. È il prezzo dell'integrazione di Internet Explorer in Windows.*

Ma così non mi funziona più niente!

Potreste obiettare che disattivando questi linguaggi, soprattutto Javascript, quasi tutti i siti Web diventano inutilizzabili. Avete perfettamente ragione.

Il mio consiglio non è di disattivarli *per sempre*: è di tenerli disattivati *salvo necessità,* riattivandoli soltanto quando serve e quando vi fidate del sito che vi obbliga a riattivarli.

In altre parole, usate un browser che vi consente di attivare e disattivare al volo questi linguaggi (Opera, per esempio) e teneteli disattivati durante la normale navigazione; se vi imbattete in un sito usabile solo attivando questi linguaggi, chiedetevi se vi potete fidare; riattivate questi linguaggi soltanto se la risposta è un *Sì* convinto e disattivateli quando cambiate sito.

Tenete presente che **se girate per Internet lasciando attivati Javascript e soci, è sufficiente visitare per sbaglio un sito-trappola per infettarsi**.

Siti attendibili

Potete aggirare il problema dei siti che non funzionano ricorrendo all'area *Siti attendibili* che trovate nella scheda Protezione di Internet Explorer. Se la selezionate e poi cliccate su *Siti*, potete memorizzare il nome del sito di cui volete fidarvi (ma mi raccomando, fatelo solo per i siti strettamente indispensabili).

A quel sito, **e soltanto a quel sito**, verrà concessa massima fiducia (la protezione è *Bassa*) e tutto funzionerà, mentre tutti gli altri siti continueranno a essere bloccati dalla protezione *Alta*. Per alcuni siti fidati può essere necessario disattivare l'opzione *Richiedi verifica server.*

> *Potete specificare anche soltanto una parte del nome del sito, in modo da includere tutte le sue sezioni: per esempio, se specificate* microsoft.com, *anche* windowsupdate.microsoft.com *verrà gestito come "sito attendibile".*
>
> *Ricordate di includere fra i siti attendibili quello della vostra banca, dei negozi online che utilizzate e delle società produttrici di antivirus di cui adoperate i servizi di scansione "senza installazione" contro i virus.*

Altre difese contro i linguaggi a rischio

Le tecniche descritte fin qui irrobustiscono Internet Explorer e gli altri browser, ma cosa succede se un file contenente uno di questi microprogrammi entra nel vostro computer attraverso un canale diverso dal Web, per esempio su un CD prestatovi da un amico?

Un primo passo molto efficace è riassegnare al Blocco Note le estensioni dei file contenenti questi microprogrammi, come descritto nel Capitolo 3; ma conviene togliere completamente a Windows la possibilità di eseguire i più pericolosi, quelli di tipo VBS (*Visual Basic Scripting*), disattivando il cosiddetto *Windows Scripting Host* e riattivandolo soltanto se strettamente necessario.

Symantec offre gratuitamente un programma, *Noscript.exe* (*www.symantec.com/avcenter/venc/data/win.script.hosting.html*), che provvede a questa bisogna. È sufficiente scaricarlo ed eseguirlo facendo doppio clic sulla sua icona.

In alternativa, potete semplicemente cancellare o rinominare il componente di Windows incaricato di eseguire i programmi VBS, di nome *wscript.exe*, che potete trovare usando la funzione Cerca del menu Start.[76]

Blindare i browser alternativi

Come dicevo, in alcune circostanze anche i browser alternativi possono essere vulnerabili a questi microprogrammi annidati nelle pagine Web. Molti di questi browser risolvono drasticamente il problema perché sono incapaci di riconoscere (e quindi eseguire) alcuni tipi di microprogrammi, per esempi, ActiveX o VBS, ma talvolta accettano quelli Javascript e Java.

Imparate pertanto a disattivare l'esecuzione automatica di questi microprogrammi e ad attivarla soltanto se visitate un sito affidabile che lo richieda. La procedura esatta dipende dal browser che usate.

Per esempio:

- In Opera è sufficiente premere il tasto F12 e scegliere le opzioni *Java* e *Javascript*; Opera non gestisce né ActiveX, né Visual Basic Scripting, per cui non occorre fare altro.
- In Mozilla non c'è supporto per ActiveX e Visual Basic Scripting; Java si disabilita tramite *Modifica* > *Preferenze*

> *Avanzate*, disattivando la casella *Abilita Java*; Javascript si disabilita nello stesso sottomenu *Avanzate*, cliccando sulla sezione *Script e plug-in* e disattivando le caselle *Navigator* e *Posta e gruppi di discussione* sotto *Attiva Javascript*.

- In Firefox, scegliete *Strumenti* > *Opzioni* > *Proprietà Web* e disattivate *Abilita Java* e *Abilita Javascript*. Anche in questo browser, ActiveX e VBS non sono gestiti.

  Ricordate che molti siti usano Javascript anche per frivolezze come la gestione dei menu, esponendovi a un rischio inutile per ragioni puramente estetiche e causando non pochi problemi ai disabili che usano Internet.

  Navigando con Javascript disattivato, questi menu ovviamente non funzionano. In tal caso, se vi fidate del sito, vi tocca attivare l'esecuzione di Javascript. Se invece non vi fidate del sito, cambiate sito!

Avrete notato che nessuno dei browser alternativi elencati gestisce ActiveX e Visual Basic Scripting. Non è che non sono all'altezza di farlo: è una limitazione voluta. Questi sono infatti i linguaggi più pericolosi e quindi abusati.

Ma il sito Web di Microsoft usa ActiveX e VBS a piene mani, per esempio per gli aggiornamenti di Windows. Allora che si fa? Semplice: **visitate il sito Microsoft usando Internet Explorer.** È uno dei rari casi in cui ci si può fidare a usare il browser Microsoft. Del resto, se non vi fidate del sito Microsoft, perché state ancora usando Windows?

Il browser mascherato

Come già accennato, alcuni siti Web funzionano soltanto con Internet Explorer. In realtà spesso funzionerebbero anche con gli altri browser, ma contengono un filtro che identifica il browser usato dall'utente e lo bloccano se è diverso da Internet Explorer.

Questo viene fatto, ufficialmente, per "evitare problemi di sicurezza"; in realtà è spesso una questione di pigrizia e incompetenza dei creatori del sito. Basterebbe rispettare gli standard ufficiali di Internet, definiti da un organismo super partes (il *World Wide Web Consortium* o *W3C*, *www.w3.org*), come fanno i browser alternati-

vi, ma siccome Internet Explorer è il browser più diffuso, lo si usa come pseudostandard, falle comprese.

Di conseguenza, i browser alternativi si sono fatti furbi: sono in grado di annunciarsi a questi siti dicendo di essere Internet Explorer. Questo semplicissimo espediente consente quasi sempre di scavalcare i filtri di identificazione e quindi usare i browser alternativi al posto di Internet Explorer anche dove in teoria non si potrebbe.

Per esempio, se usate Opera (che rispetta gli standard, come gli altri browser alternativi) e vi imbattete in un sito che dice *"spiacente, ma il suo browser non è compatibile"*, provate a premere F12 e scegliere dal menu il browser che volete imitare (Figura 11.3). Il fatto che i browser alternativi sovente funzionino lo stesso con questi siti dimostra la suddetta pigrizia e incompetenza.

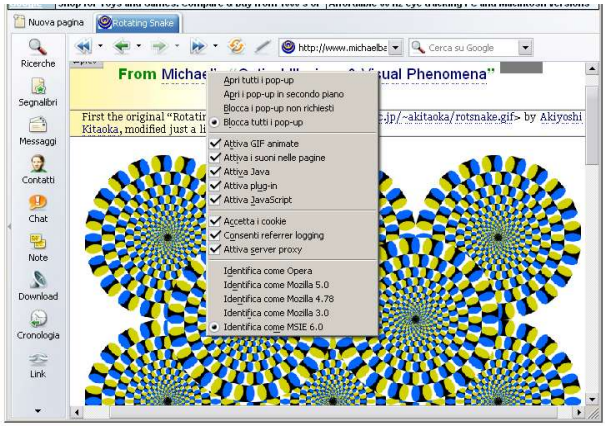

Figura 11.3

Uso sicuro del Web

Conquistare un livello ragionevole di sicurezza informatica non dipende soltanto dall'uso di strumenti tecnici adeguati: richiede anche un'abbondante dose di un ingrediente che non si compra in negozio: il buon senso.

Ora che vi ho dato qualche dritta su come rendere meno difettosi i vostri strumenti, è importante che teniate comunque un comporta-

mento cauto quando girate per la Rete. Alcune cautele, però, non sono affatto intuitive, per cui è meglio che ne parliamo un attimo.

Non siete invincibili

Anche se avete tribolato non poco nelle pagine precedenti per correggere le magagne di Windows, non è assolutamente il caso di buttare al vento ogni preoccupazione. Evitate comunque di visitare siti dedicati al software pirata (i cosiddetti *warez* e affini), quelli per adulti e quelli che offrono (o fanno credere di offrire) musica MP3 o loghi e suonerie "gratis".

Questi siti, infatti, sono quasi sempre gestiti da professionisti della truffa e dell'intrusione informatica, che possono facilmente bucare le vostre difese (benché più robuste della media) o indurvi ad abbassarle con espedienti psicologici. A volte anche siti dedicati a temi meno chiaramente controversi tendono trappole di questo tipo, ma la concentrazione maggiore di pericoli è in quelli che ho citato.

Occhio al lucchetto

Quando interagite con un sito nel quale dovete immettere dati personali (indirizzo, numero di carta di credito per acquisti, eccetera), assicuratevi che la comunicazione sia **cifrata**, altrimenti chiunque può intercettare i vostri dati e usarli per derubarvi.

La cifratura della comunicazione si può verificare in due modi molto semplici:

- nella barra di navigazione, l'indirizzo deve iniziare con *https* invece che con *http* (aiuto mnemonico: S come *Sicurezza*);
- nella finestra del browser c'è un'icona di un lucchetto, che deve essere in posizione chiusa.

Controllate che siano presenti *entrambi* questi indicatori. Non affidate **mai** dati personali economici (numero di conto corrente o di carta di credito) a siti che non esibiscono *https* e lucchetto chiuso quando ve li chiedono. Nessun commerciante serio fa a meno di cifrare la transazione di pagamento.

> *Tenete presente, però, che esistono modi per visualizzare fraudolentemente questi due indicatori. Di conseguenza, la loro presenza da sola* ***non garantisce***

*l'autenticità del sito, ma la loro assenza **garantisce** che qualcosa non va.*

Guardare prima di cliccare

Prima di cliccare su un link in una pagina Web, mettetevi sopra il cursore del mouse e guardate se la finestra del browser indica da qualche parte l'indirizzo al quale verrete portati se cliccate. Quasi tutti i browser, sia Internet Explorer sia gli alternativi, visualizzano quest'informazione, utilissima per smascherare burle e trappole.

Se l'indirizzo inizia con dei numeri invece che con un nome (per esempio *http://212.125.42.47*) o termina con un'estensione di quelle eseguibili (per esempio *exe* e le altre citate nei capitoli precedenti), diffidatene: probabilmente è un trucco per indurvi a scaricare ed eseguire un virus o peggio.

Tenete presente, però, che esistono molti altri modi per mascherare l'indirizzo, per cui questa tecnica difensiva è utilizzabile soltanto come test *positivo*, ossia consente soltanto l'identificazione certa di un pericolo senza garantire la sua assenza.

In altre parole, se l'indirizzo rivelato ha qualche caratteristica sospetta, consideratelo quasi sicuramente pericoloso: ma se non ne ha, non consideratelo sicuramente innocuo.

Senza diventare paranoici, prendete semplicemente l'abitudine di dare un'occhiata all'indirizzo di destinazione visualizzato: può essere un indizio prezioso in più per difendersi.

Siete davvero dove credete di essere?

È facile far credere a chi naviga in Rete di essere in un certo sito quando in realtà è altrove. Al livello più semplice, si usa un indirizzo visivamente simile a quello desiderato dall'utente, come *www.whitehouse.com* (esiste veramente, ma non è la Casa Bianca, che è *whitehouse.gov*) o *www.bancalntesa.it* (dopo *banca* c'è una L, non una I).

Tuttavia è anche abbastanza facile beffare direttamente il browser:

- gli si può far visualizzare nella barra dell'indirizzo un indirizzo diverso da quello che state effettivamente visitando;

- si può inviare in un e-mail un link che apparentemente appartiene a un sito fidato ma in realtà conduce altrove (il link visualizzato non corrisponde al link effettivo);[77]
- si può indurre il browser a inserire, nella schermata di un sito Web autentico, una pagina che proviene da un sito ostile.[78]

Niente panico! Il rimedio è molto semplice:

> ***Regola 9: Non fidatevi dei link a banche o negozi forniti da sconosciuti.*** *Possono essere falsi e portarvi a un sito-truffa. Usate invece i Preferiti o il copia-e-incolla, oppure digitateli a mano, in un browser sicuro.*

In altre parole:

- usate un browser diverso da Internet Explorer e tenetelo aggiornato (in modo che sia il più sicuro possibile);
- se dovete visitare un sito commerciale o quello della vostra banca, non cliccate su un link che vi ha dato qualcuno di cui non conoscete con certezza l'identità (per esempio un link trovato in un e-mail, il cui mittente è notoriamente falsificabile);
- copiate e incollate nel browser il testo *visibile* del link (che può essere diverso da quello che in realtà vuol farvi visitare l'aggressore) e guardate se il nome del sito è scritto esattamente;
- se il link contiene caratteri anomali che servono per mascherarne la vera destinazione (per esempio chioccioline e simboli di percentuale), il browser sicuro se ne accorgerà e vi avviserà;
- per il massimo della sicurezza, memorizzate gli indirizzi dei vostri siti commerciali o bancari nei Preferiti del browser e accedete a quei siti soltanto tramite i Preferiti oppure digitando a mano i loro indirizzi.

Per esempio, se ricevete da *servizioclienti@bancadirorna.it* l'invito a reimmettere i vostri codici di accesso visitando il sito della banca tramite il link gentilmente fornito, ossia *www.bancadirorna.it/accesso.htm*, non abboccate: digitate *a mano* il nome del sito, in modo da collegarvi sicuramente al sito reale. Il link fornito, infatti, è fasullo. Dove? Guardate bene com'è scritto *"rorna"*. Sono cinque lettere, non quattro.

Tornerò su questo genere di truffe e sul problema dei link-trappola anche nel prossimo capitolo, perché spesso coinvolgono anche le vulnerabilità dell'e-mail.

Come collaudare il browser: dialer

Volete una prova tangibile del miglior funzionamento dei browser alternativi rispetto a Internet Explorer? Allora trovate un amico o un collega che non sia convinto della vulnerabilità di Internet Explorer e lo usa ancora allo stato brado (ossia senza blindarlo come descritto nelle pagine precedenti) e invitatelo a visitare insieme a voi un sito che offre a pagamento immagini di celebrità più o meno spogliate, senza arrivare al porno. Non è difficile trovarne uno di questi siti tramite Google. Ditegli che sapete che è un compito ingrato, ma è a fini strettamente educativi.

È facile che troviate, frugando in questi ambienti, un sito che contiene un dialer di quelli descritti nel Capitolo 8. Quando lo trovate, visitate entrambi *soltanto la sua pagina iniziale*, *senza cliccare nulla*: assicuratevi che la vostra cavia scettica usi Internet Explorer, mentre voi usate un browser alternativo.

Noterete subito la differenza di comportamento e di sicurezza fra i due browser:

- Con Internet Explorer "al naturale", anche se completamente aggiornato (eccetto il Service Pack 2, descritto a fine capitolo) e con i normali livelli di protezione, comparirà un *"Avviso di protezione",* che avviserà in modo poco chiaro sui costi del servizio e vi inviterà a cliccare su *Sì* (Figura 11.4). L'invito, naturalmente, non va accettato.
  Cliccando su *Sì,* verrebbe installato automaticamente il dialer, con conseguente rischio in bolletta. Cliccando su *No*, l'avviso-invito continuerà a comparire e ci vorranno diversi *No* per farlo smettere. Insistente, vero?

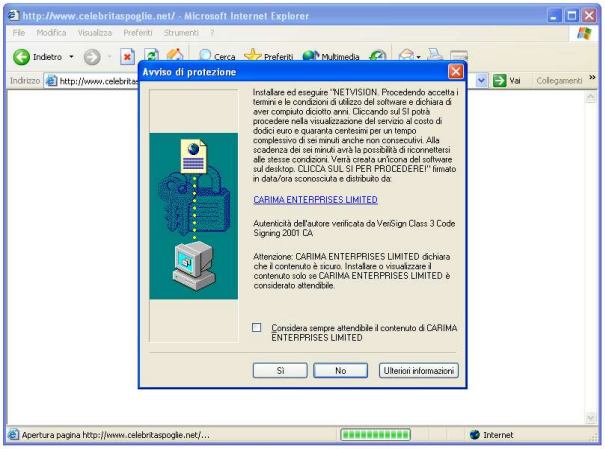

Figura 11.4

- Con un browser alternativo, per esempio Firefox (Figura 11.5), otterrete la schermata iniziale del sito, ma nessun enigmatico "avviso di protezione": più semplicemente, se proverete a cliccare sui link presenti nel sito (che vorrebbero lanciare il dialer), **non succederà nulla**. I browser alternativi, infatti, non riconoscono gli avvisi di protezione e quindi tolgono ai dialer il loro canale d'attacco preferenziale.
  In altre parole, usando un browser alternativo potrete infettarvi con un dialer **soltanto se lo scaricate e lo eseguite intenzionalmente.** Non basta cliccare per sbaglio su un *Sì*.
  Questo è particolarmente utile quando si teme che chi usa il computer non sia sempre attento ai dettagli dei messaggi a video che avvisano dei costi del servizio (per esempio i giovani e i meno giovani ancora in piena tempesta ormonale).

Potete usare il sito sparadialer anche per verificare l'efficacia delle misure di irrobustimento di Internet Explorer che vi ho consigliato: se l'avete aggiornato (senza includere il Service Pack 2) e anche "blindato" con la protezione *Alta*, non vedrete l'avviso di protezione, ma otterrete un messaggio secondo il quale *"le impostazioni di protezione correnti non consentono l'esecuzione dei controlli ActiveX... la pagina potrebbe non essere visualizzata correttamente"* (Figura 11.6). Infatti la schermata è completamente vuota e lo rimane anche cliccando su *OK*. E così dev'essere.

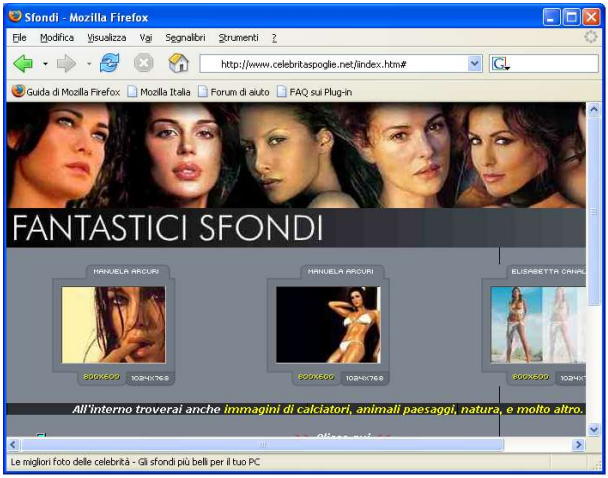

Figura 11.5

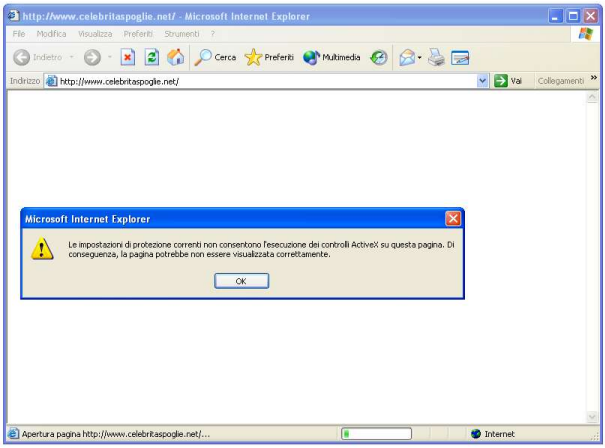

Figura 11.6

Altri collaudi

I siti dedicati alla sicurezza abbondano di test con i quali potete cimentarvi e verificare quanto è sicuro (o insicuro) il vostro browser.

Alcuni di questi test sono stupefacenti; altri sono divertenti anche come scherzi da fare agli amici che si ritengono informatici provetti. Troverete che anche i browser alternativi non sono perfetti e che bisogna sempre tenere sveglio il cervello per tenerli in riga.

Purtroppo molti di questi siti sono in inglese:

- *Browserspy* (*gemal.dk/browserspy*);
- *Guninski.com;*
- *PC Flank* (*www.pcflank.com*);
- *Qualys Browser Check* (*browsercheck.qualys.com*);
- *Secunia* (*www.secunia.com*) offre sia gli elenchi delle falle ancora aperte e le relative dimostrazioni, sia un test specifico per mostrare quante informazioni vengono divulgate dal vostro browser (*https://testzone.secunia.com/browser_checker/*).

In italiano potete invece dilettarvi con *Salvatore Aranzulla's Lab* (*mirabilweb.altervista.org/test_browser/index.htm*) e con la mia piccola galleria di test, denominata *Browser Challenge*, su *www.attivissimo.net*.

Cosa cambia con il Service Pack 2

Anche Internet Explorer beneficia delle migliorie offerte dal Service Pack 2. Non c'è molto di nuovo che non ci sia già nei browser concorrenti (e il *tabbed browsing* rimane gravemente assente), ma si tratta comunque di[79] un gradito passo in avanti.

Meno spot, grazie

Internet Explorer, infatti, recupera un po' del distacco inflittogli dai browser alternativi mettendo finalmente a disposizione degli utenti un "ammazza-*popup*", ossia un'opzione che gli permette di bloccare automaticamente tutte le petulanti finestre pubblicitarie che si aprono visitando certi siti e che a volte mandano in tilt il computer.

L'opzione per bloccare i popup è nel menu Strumenti ed è regolabile su vari livelli, in modo che non blocchi per esempio i popup usati per gestire lo scaricamento da certe biblioteche di programmi di Internet ma stronchi sul nascere i popup di pura pubblicità. Se c'è qualche sito del quale vi serve vedere i popup, potete specificarne il nome nelle opzioni del blocco pop-up.

Accessori pericolosi

Il Service Pack 2 inoltre introduce la *Gestione componenti aggiuntivi* nel menu Strumenti di Internet Explorer. Questa nuova funzione permette di elencare, gestire e se necessario rifiutare i programmi aggiuntivi per il browser Microsoft presenti nel computer.

I programmi aggiuntivi comprendono un po' di tutto: si va dalle barre di navigazione che facilitano l'uso di Internet Explorer ai veri e propri spyware, passando per i *controlli* (microprogrammi) ActiveX. Con il Service Pack 2 diventa molto più semplice eliminarli: li selezionate dall'elenco e scegliete *Disattiva*. Una volta riavviato Internet Explorer, il componente aggiuntivo non viene più usato.

Avvisi più chiari, criteri più sicuri

Anche con la protezione impostata a *Media*, Internet Explorer impara a essere meno amicone di tutti dopo che avete installato il Service Pack 2. Per esempio, i siti "sparadialer" vengono bloccati in modo molto più esplicito: l'infingardo "avviso di protezione" non compare, come avviene con i browser alternativi.

Al suo posto viene visualizzata una barra informativa (Figura 11.7): se vi cliccate sopra, però, è ancora possibile installare il controllo ActiveX e quindi aprire la strada al dialer (anche se il menu di opzioni che compare contiene anche una voce *Quali rischi si corrono*). Questo è un pericolo al quale i browser alternativi non vi espongono.

Se cliccate sulla scelta che consente di installare il controllo ActiveX, compare l'avviso di protezione, ma in una forma più concisa di quella pre-Service Pack 2, che **nasconde le già scarse informazioni sui costi di connessione**. In compenso, però, consente anche di bloccare permanentemente i controlli ActiveX delle singole società sparadialer.

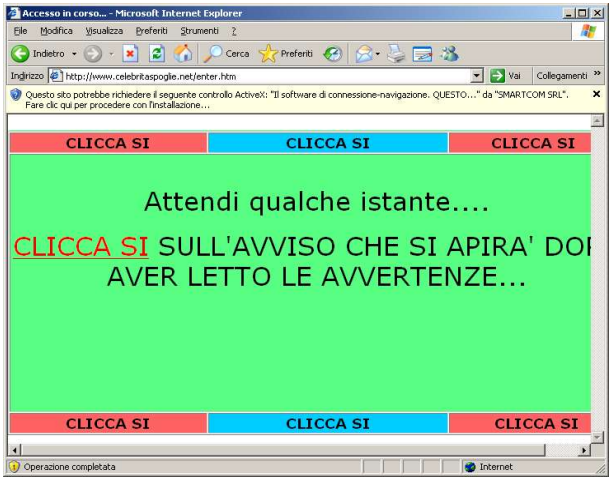

Figura 11.7

Altri affinamenti di Internet Explorer

Anche l'identificazione del tipo di file scaricato, classica debolezza di Windows e Internet Explorer ampiamente sfruttata dagli aggressori, diventa più prudente dopo il Service Pack 2: in pratica, è molto più difficile ricevere un virus travestito da file audio, per esempio.[80]

Il Service Pack 2, inoltre, toglie automaticamente tutti i privilegi di esecuzione all'area Risorse del Computer. Di conseguenza, se un aggressore riesce a ingannare Internet Explorer e fargli credere che le pagine ostili del suo sito originano dall'area Risorse del Computer, Internet Explorer non ne eseguirà i contenuti pericolosi.

Meno insicuro, ma usabile?

Indubbiamente Microsoft ha fatto un notevole sforzo per cercare di aggiornare Internet Explorer alle moderne esigenze di funzionalità e di sicurezza, ma c'è ancora molta strada da fare. I browser alternativi, anche se non perfetti, danno tuttora maggiori garanzie di sicurezza nella navigazione in Rete.[81]

Capitolo 12
Posta blindata

Indovinate qual è il metodo preferito dagli aggressori per infettare un computer? Esatto: la posta elettronica.

È così facile: basta allegare un virus a un e-mail, dare al messaggio un titolo accattivante (tipo *"Ecco le tue foto!"* oppure *"Il salvaschermo di Britney Spears che mi chiedevi"*) e il destinatario quasi sicuramente aprirà incuriosito l'allegato e s'infetterà. Come rubare caramelle a un bambino.

Si può fare anche di meglio: se la vittima usa programmi vulnerabili, un e-mail opportunamente confezionato può eseguire *spontaneamente* l'allegato, senza l'intervento della vittima.

Anche la truffa corre via e-mail. Le varie offerte di Viagra, siti pornografici e altri prodotti e servizi miracolosi a prezzi stracciati non sono soltanto una scocciatura: sono crimini. Oltretutto rischiano di appestarvi lo schermo di immagini imbarazzanti.

L'e-mail veicola anche tentativi di rubarvi denaro dal conto corrente, tramite messaggi la cui grafica simula perfettamente quella della vostra banca, ma che in realtà trasmettono i vostri codici di accesso al conto a un malfattore.

Ci sono insomma delle ottime ragioni per rendere più sicuro l'uso della posta elettronica. E la sicurezza, come al solito, non si basa soltanto sulla tecnologia ma richiede anche un po' di buon senso.

Cominciamo dalla tecnologia, perché è inutile avere buon senso se veniamo traditi dallo strumento: e purtroppo Outlook Express, il popolarissimo programma per la gestione dell'e-mail che Microsoft ci fa trovare preinstallato in Windows, è uno strumento che tradisce facilmente.[82]

Molti dei più diffusi problemi di sicurezza riguardanti la posta sono risolvibili semplicemente rimpiazzando Outlook Express. Da questo discende la già citata Regola 6:

> ***Regola 6: Non usate Internet Explorer e Outlook Express.*** *Sostituiteli con prodotti alternativi più sicuri.*

Avete blindato Internet Explorer nel capitolo precedente (l'avete fatto, vero?): ora tocca al secondo elemento del duo, perché **purtroppo anche Outlook Express, come Internet Explorer, è estremamente vulnerabile** e oltretutto le sue vulnerabilità sono quelle preferite dagli aggressori informatici, perché sono facili da sfruttare e possono fare un elevatissimo numero di vittime a causa della larghissima diffusione del programma.

Capisco che non tutti siano disposti a cambiare programma di gestione della posta; è sempre brutto dover cambiare abitudini. So anche che in molte situazioni non si può abbandonare Outlook Express perché c'è un ordine dall'alto oppure per ragioni di compatibilità con servizi che funzionano soltanto con Outlook Express (tipicamente si tratta, guarda caso, di servizi Microsoft). Per questo ho preparato anche una sezione di questo capitolo dedicata all'irrobustimento di Outlook Express, per la serie "piuttosto che niente, meglio piuttosto".

Vi assicuro, comunque, che tribolerete molto meno cambiando programma che cercando di raddrizzare Outlook Express.

Cambiare programma di posta

Se state leggendo questa sezione, ho una cosa importante da dirvi: *Bravi!* Avete deciso di prendere il toro per le corna: niente mezze misure. Non ve ne pentirete. Quando sentirete gli altri raccontare le loro tragedie con virus e truffe, voi potrete sorridere. Non troppo sfacciatamente, però; non sta bene.

Ecco un breve elenco dei più popolari programmi di posta alternativi: tutti soddisfano i requisiti di sicurezza necessari per un uso sereno dell'e-mail se opportunamente configurati, ma differiscono fra loro in quanto a prestazioni e modo di interagire con l'utente.

Visivamente, alcuni somigliano moltissimo a Outlook Express, senza però averne le manchevolezze. Inoltre, siccome sono meno diffusi dei prodotti Microsoft, le loro eventuali falle sono oggetto di minori attenzioni da parte degli aggressori informatici. Sono quasi tutti disponibili anche in versione gratuita e in italiano, e questo di certo non guasta.

- **Eudora** (*www.eudora.com*), gratuito in versione semplificata in inglese; disponibile in italiano soltanto in versione completa a pagamento (*www.eudora.com/sales/localized.html*).

- **The Bat!** (*www.ritlabs.com*), a pagamento, disponibile anche in italiano (*www.ritlabs.com/en/purchase/regional_dealer.php#Italy*).
- **Pegasus Mail** (*www.pmail.com*) gratuito, in inglese con istruzioni italiane presso *www.pegasusmail.tk*.
- **Foxmail** (*web.tiscali.it/alexseb/fox/*), gratuito e disponibile in italiano; il sito originale è *fox.foxmail.com.cn.*
- **Thunderbird** (*www.mozillaitalia.org*), gratuito e disponibile in italiano; il sito originale è *www.mozilla.org*.

> Sul mio sito *www.attivissimo.net*, nella sezione dedicata a questo libro, trovate le istruzioni dettagliate per scaricare, installare e configurare Thunderbird, il programma che uso su tutti i miei computer Windows, Linux e Mac.

Posta senza programma: Webmail

Oltre alle alternative che ho elencato qui sopra ce n'è anche un'altra: fare completamente a meno di un programma per gestire la posta. Questo risultato apparentemente impossibile si ottiene usando la cosiddetta *Webmail*, ossia una casella di posta con la quale si interagisce usando un comune browser.

Quasi tutti i fornitori di accesso a Internet offrono la Webmail gratuitamente ai propri clienti: probabilmente l'avete già disponibile e non lo sapete. Ci sono anche società che regalano la Webmail senza essere fornitori d'accesso, come fa per esempio Google (Figura 12.1) con Gmail (*gmail.google.com*).

La Webmail è una soluzione molto pratica per certi versi e molto scomoda per altri:

- da un lato, consente di accedere alla propria posta da qualsiasi computer del mondo immettendo i giusti codici segreti d'accesso (ideale quando si viaggia);
- dall'altro, obbliga a stare collegati a Internet mentre si consulta la propria casella. Se pagate la connessione Internet a tempo, i costi salgono in fretta; e se per qualsiasi ragione non potete collegarvi a Internet, tutta la vostra posta è inaccessibile. Usando un programma, invece, la posta scaricata e spedita risiede tutta sul vostro PC ed è consultabile in qualsiasi momento.

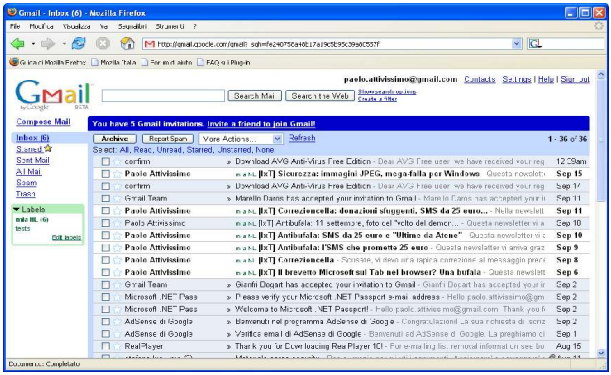

Figura 12.1

Usare la Webmail ha numerosi vantaggi in termini di sicurezza, ma non è l'ideale. È **difficile, ma comunque possibile, infettarsi dalla Webmail** se la consultate con un browser vulnerabile; inoltre di norma il contenuto grafico dei messaggi non viene filtrato, per cui possono arrivare comunque immagini indesiderate e inadatte. È comunque notevolmente più sicuro che usare Outlook Express allo stato brado.

Programmi di posta integrati nei browser

Alcuni browser, come per esempio Opera e Mozilla, includono anche la gestione della posta. Di primo acchito integrare le due funzioni può sembrare una buona idea, ma l'integrazione comporta il rischio che una falla nel browser causi problemi nella gestione della posta e viceversa, come sciaguratamente è avvenuto per la coppia Internet Explorer/Outlook Express.

Conviene insomma tenere separate le due funzioni e dare istruzioni al browser di passare gli indirizzi di posta trovati nelle pagine Web al programma che gestisce l'e-mail e viceversa dire al programma per l'e-mail di passare al browser gli indirizzi dei siti trovati nei messaggi di posta. Questo produce gli stessi effetti dell'uso di un programma integrato senza comportarne i rischi.

Migrare senza perdere nulla

Una delle principali preoccupazioni di chi decide di cambiare programma per la gestione dell'e-mail è la perdita dell'archivio dei messaggi e della rubrica degli indirizzi.

In realtà, praticamente tutti i programmi alternativi a Outlook Express sono in grado di acquisire (tecnicamente si dice *importare*) gli archivi di posta e la rubrica del programma Microsoft. Come sempre, **conviene fare un backup del proprio archivio** e fare qualche esperimento, ma in genere non ci sono problemi.

> *Cambiare programma per l'e-mail non comporta cambiare il proprio indirizzo di posta. Basta immettere nel programma nuovo i parametri immessi in quello vecchio e dire a quello nuovo di diventare il programma di posta predefinito.*

Migrare, insomma, si può: ma come si fa a scegliere un programma di posta più sicuro o irrobustire Outlook Express? Ci sono alcuni criteri tecnici di base da seguire, ma non va trascurata la praticità d'uso, che è spesso questione di gusti e di abitudini.

Criteri di sicurezza

Fondamentalmente, i criteri di sicurezza per la posta sono due, validi sia per chi resta fedele a Outlook Express, sia per chi cambia programma, e riassumibili in una singola frase:

> *Un programma di e-mail sicuro deve visualizzare esclusivamente il testo dei messaggi, senza usare effetti grafici, senza eseguire istruzioni nascoste, senza visualizzare immagini e senza aprire automaticamente allegati.*

Detto così sembra un comandamento un po' da talebano: perché bisogna rinunciare alle immagini, agli sfondi, alle animazioni e alle musichette di sottofondo? Perché bisogna rinunciare persino ai tipi di carattere e ai grassetti? La posta così spartana è *deprimente!*

Per capire l'importanza di queste rinunce occorre esaminarne singolarmente le ragioni.

Testo puro e semplice

Quando nacque, l'e-mail era simile a un telegramma: non si poteva scegliere il tipo di carattere, non si potevano definire parole sottolineate o in grassetto o in corsivo e non si potevano definire sfondi colorati per i messaggi. Di cagnolini scodinzolanti o modelle sculettanti, ovviamente, non se ne parlava proprio.

Si poteva trasmettere, insomma, soltanto il testo nudo e crudo: quello che gli informatici chiamano *ASCII* e pronunciano *"àschi"* (sì, come la razza di cani). Per emulare certi effetti grafici si ricorreva a espedienti: per esempio, la sottolineatura era espressa *_così_* e il grassetto **così**. Gli utenti più creativi componevano grechine e addirittura "disegni" usando i simboli della tastiera (Figura 12.2). Ci si arrangiava con poco, insomma, e forse si badava di più alla sostanza.

Figura 12.2

Un bel giorno qualcuno (lasciamo stare chi) decise che c'era un modo per abbellire questi messaggi così grigi: usare lo stesso linguaggio usato per le pagine Web, ossia l'HTML.[83] Questo permetteva di annidare nei messaggi dei codici invisibili, per esempio *<B>* e *</B>* per indicare inizio e fine del grassetto.

I programmi di posta adottarono rapidamente questo sistema. Ma ben presto si pensò che si poteva fare di meglio: usare lo stesso metodo per includere nel testo anche le immagini. E già che ci siamo, perché non includere anche delle animazioni, delle musichette... e magari anche dei *programmini che si eseguono da soli?*

Avete probabilmente intuito dove sto andando a parare. **Introducendo tutti questi codici nascosti, la posta è diventata vulnerabile:**

- La possibilità di includere immagini si è presto tradotta nella comparsa automatica di pubblicità pornografica sullo schermo.

- La possibilità di includere programmi è stata sfruttata per disseminare virus, non come allegati, ma *direttamente nel testo del messaggio*. È diventato possibile infettarsi semplicemente leggendo un e-mail.[84]
- I codici nascosti hanno permesso di creare messaggi che comunicano con il proprio padrone ogni volta che vengono letti (i cosiddetti *web bug*), costituendo un vero e proprio sistema di tracciamento degli utenti.
- Grazie ai codici nascosti, si può includere in un e-mail un *link* (collegamento) che sembra portare a un sito ma in realtà porta altrove: per esempio, un truffatore fa visualizzare nel messaggio un link a *www.bancomat.it* che però porta al suo sito-trappola, indistinguibile da quello vero.

L'unico modo efficace per difendersi da tutto questo è **non eseguire eventuali istruzioni nascoste.**

Ecco il motivo della Regola 10 del Dodecalogo:

> ***Regola 10. Rifiutate la posta in formato HTML e non mandatela agli altri.*** *Usate il testo semplice, molto più sicuro.*

Se preferite una forma più diretta:

> ***La posta HTML è male; la posta di puro testo è bene.***

Se il programma di posta non esegue istruzioni nascoste nei messaggi, in un sol colpo si eliminano alla fonte tutti i rischi connessi a pornografia e pubblicità grafica indesiderata, oltre alla maggior parte delle truffe e dei virus annidati nei messaggi.

Tuttavia, siccome c'è ancora tanta gente che usa la posta HTML, un programma di posta sicuro deve anche essere in grado di **gestire in modo non pericoloso messaggi contenenti codici nascosti**, per esempio visualizzandone soltanto la parte di puro testo e ignorando i codici.

Certo, tutto questo significa rinunciare in gran parte agli effetti speciali. Così è la vita.

> *Per ridare un po' di vivacità ai messaggi, scegliete un tipo di carattere "non proporzionale" (in cui tutti i simboli hanno la stessa larghezza), come il Courier. In questo modo potrete godervi le "firme" grafiche dei tanti utenti*

della Rete che usano ancora gli effetti vecchio stile (Figura 12.3). Se usate un carattere proporzionale, l'effetto grafico viene rovinato.

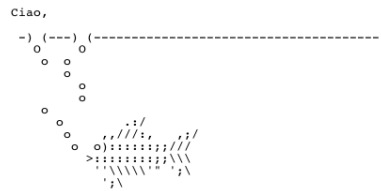

Figura 12.3

Allegati automatici

Non esistono categorie sicure di allegati. È una credenza molto diffusa, ma in realtà è facilissimo ingannare Windows e far sembrare che un allegato sia innocuo quando è in realtà un virus o un altro programma ostile. Anche un'immagine può veicolare un virus: e anche se non lo veicola, non è opportuno che venga visualizzata automaticamente. E se fosse un'immagine pornografica? *"Mamma, cosa stanno facendo quei due.... no, tre... e la capra?"*.

Di conseguenza, qualunque programma di posta che apra automaticamente gli allegati, anche soltanto quelli teoricamente innocui come le immagini (che poi non è detto che lo siano, come dicevo), è un rischio.

Un programma di posta sicuro:

- **deve ignorare completamente gli allegati**, di qualunque tipo siano o sembrino essere, ma evidenziarne la presenza;
- se gli chiedete di aprirli, **deve rifiutarsi e proporvi di salvarli** in un'apposita cartella del disco rigido, senza aprirli o eseguirli, in modo che possiate controllarli con l'antivirus e **poi** eventualmente aprirli (se lo ritenete opportuno) usando il metodo sicuro *"Apri con"* descritto nel Capitolo 3.

Sono pochi i programmi alternativi (e gli utenti) che rispettano alla lettera queste regole. La tentazione di cedere all'orpello è troppo forte e non è certo monopolio Microsoft: se passate a un programma di posta diverso da Outlook Express, quindi, preparatevi co-

munque a reimpostarlo (e reimpostarvi) secondo questi criteri di sicurezza.[85] È comunque un procedimento molto più semplice che cercare di rieducare Outlook Express.

Rinforzare Outlook Express

La prima cosa da fare per rendere Outlook Express meno insicuro è **aggiornarlo** alla versione più recente, usando per esempio Windows Update. In questo modo vi sbarazzerete perlomeno delle sue vecchie falle, ben note agli aggressori. È per questo che qui trovate soltanto istruzioni relative alla versione più recente del programma, che al momento in cui scrivo è la 6.00.[86]

Blindare Internet Explorer per la posta

Il passo successivo nell'irrobustimento di Outlook Express è controllare le impostazioni di Internet Explorer. Come già accennato, infatti, i due programmi sono interconnessi, per cui se aInternet Explorer è vulnerabile, lo diventa anche Outlook Express.

Dando per fatte le impostazioni descritte nel Capitolo 11, aprite Internet Explorer e scegliete Strumenti > Opzioni Internet e la scheda Protezione. Cliccate su *Siti con restrizioni*: non vi preoccupate se Internet Explorer dice che *"non esistono siti in quest'area"*; va bene così.

Se cliccate su *Livello predefinito*, la protezione per quest'area (che viene usata da Outlook Express) dovrebbe essere impostata ad *Alta*: se non lo è, impostatela.

Se tuttavia avete particolari esigenze, per esempio un cliente o una banca vi obbligano scelleratamente a eseguire microprogrammi ActiveX o Java o Javascript inseriti nei messaggi, queste impostazioni possono essere troppo restrittive, perché bloccano automaticamente tutti questi contenuti speciali senza neppure segnalarne la presenza.

In tal caso, potete impostare alcuni parametri, che vi elenco fra un attimo, a *Chiedi conferma*: così verrete avvisati della situazione e potrete ragionarci sopra (date comunque conferma soltanto se avete ottime ragioni per farlo). Tante richieste di conferma possono però rivelarsi una scocciatura eccessiva; a voi la scelta.

Se scegliete di essere avvisati, impostate a *Chiedi conferma* soltanto i seguenti parametri, cliccando su *Livello personalizzato:*

- *Esegui script controlli ActiveX contrassegnati come sicuri*
- *Download dei caratteri*
- *Invia dati modulo non crittografati*[87]
- *Trascina o Copia e Incolla file*[88]
- *Visualizza contenuto misto*[89]

Gli altri parametri vanno lasciati disattivati, perché riguardano situazioni che sono sicuri sintomi di un aggressore o di un incosciente e che quindi vanno bloccate senza appello.

Due altri parametri da tenere sotto sorveglianza sono *Autenticazione utente* e *Autorizzazioni al canale del software*. Il primo va impostato a *Richiedi nome utente e password*, altrimenti Windows potrebbe dare automaticamente la vostra password di accesso a Windows ai siti o agli e-mail che la richiedono; il secondo va impostato su *Protezione alta* e riguarda una tecnologia di Internet ormai in disuso ma che qualche vandalo potrebbe riesumare con intenti ostili. In ossequio al principio *"quello che non c'è non si può rompere"*, conviene togliere anche questo appiglio.[90]

Disaccoppiare Internet Explorer da Outlook Express

Alcuni programmi per la posta sfruttano Internet Explorer per visualizzare i messaggi che arrivano in formato HTML. Questo significa che se c'è una falla in Internet Explorer, il programma di posta diventa vulnerabile. **È quindi estremamente importante impedire che il programma di posta invochi Internet Explorer.** Questa è una raccomandazione che vale anche per i programmi alternativi a Outlook Express, come per esempio Eudora.[91]

Per evitare che Outlook Express si appoggi a Internet Explorer per la visualizzazione dei messaggi, andate in Outlook Express alla voce di menu *Strumenti* > *Opzioni*, scegliete la scheda *Lettura* e fate comparire il segno di spunta in *Leggi tutti i messaggi in testo normale*.[92] [93]

Se il vostro Outlook Express non ha quest'opzione, si tratta di una versione non aggiornata. Aggiornatelo, e l'opzione comparirà per magia.

Purtroppo questa modifica, estremamente importante per la sicurezza, comporta un prezzo: per motivi incomprensibili, blocca la ricerca di parole nel testo di un messaggio. Provare per credere. I programmi di posta alternativi non hanno questa eccentrica limitazione.[94]

C'è anche un'altra modifica importante da fare per separare Internet Explorer da Outlook Express. Come descritto nelle pagine precedenti, Outlook Express attinge alle Opzioni Internet (condivise con Internet Explorer) per sapere come comportarsi. In particolare, usa le "aree di protezione" già viste nel Capitolo 11.

Potrebbe sembrarvi logico che Outlook Express debba usare l'area *Internet*, visto che è da lì che arrivano i messaggi: invece deve usare l'area *Siti con restrizioni*. La corretta impostazione di Outlook Express si verifica andando in Strumenti > Opzioni > Protezione e controllando che sia selezionata appunto l'area *Siti con restrizioni*.

La ragione di questa scelta stravagante non è delle più semplici; se vi fidate del mio consiglio, potete anche fare a meno di approfondire e potete saltare i prossimi tre paragrafi.

Non vi fidate? Come volete. La ragione è che se Outlook Express usasse l'area *Internet*, adotterebbe il livello di protezione che avete definito per la navigazione nella Rete con Internet Explorer.

Se siete stati diligenti, questo livello è impostato su *Alta*, ma vi capiterà prima o poi di abbassarlo momentaneamente per interagire con qualche sito di cui vi fidate senza perdere tempo ad aggiungerlo ai siti attendibili. Se poi vi dimenticate di ripristinare il livello *Alta,* oppure non lo impostate del tutto perché lo trovate troppo penalizzante, Outlook Express abbasserà le proprie difese. Ve l'avevo detto, che non era una ragione semplice.

In estrema sintesi: assegnando a Outlook Express l'area *Siti con restrizioni*, tenete separate le impostazioni di sicurezza di Internet Explorer da quelle di Outlook Express, per cui una dimenticanza nel browser non provoca una breccia anche nel programma di posta.

Apertura prudente degli allegati in Outlook Express

Il pericolo principale dell'e-mail è costituito dai virus, e quasi tutti i virus arrivano sotto forma di allegati ai messaggi. Occorre quindi alzare qualche barriera contro gli allegati ostili.

In Outlook Express, scegliete *Strumenti* > *Opzioni* e la scheda Protezione. Troverete una casella denominata *Non consentire salvataggio o apertura di allegati che potrebbero contenere virus*.

Se la casella contiene un segno di spunta, moltissimi tipi di allegati vengono bloccati: Outlook Express li scarica, ma non è possibile aprirli.

La voce di menu che normalmente permetterebbe di aprirli nel riquadro di anteprima di Outlook Express (accessibile cliccando sull'icona del fermaglio) è infatti disabilitata e visualizzata in grigio per gli allegati ritenuti pericolosi (Figura 12.4). Se fate doppio clic sul messaggio che li trasporta ricevete l'avviso che *"è stato rimosso l'accesso ai seguenti allegati"*.

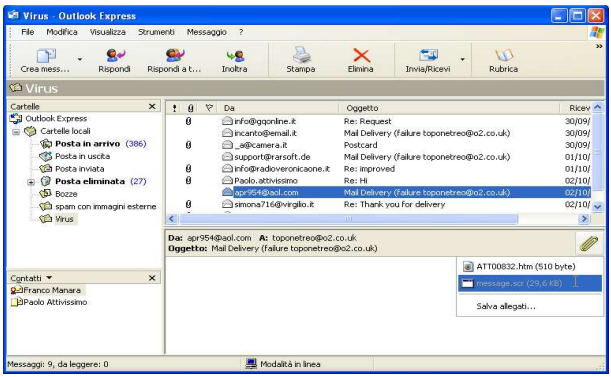

Figura 12.4

Questa sembra un'ottima cosa, perlomeno fino al momento in cui scoprite che vengono bloccati anche molti allegati *desiderati:* per esempio, se non avete installato Microsoft Office, vengono bloccati anche i file di Word.[95] Stessa sorte tocca ai file PDF, così usati per lo scambio di documenti, se non avete installato il relativo programma di lettura gratuito (Acrobat Reader). Invece immagini e file compressi (ZIP) sono apribili senza problemi. Cosa sta succedendo?

Semplice: quest'opzione di Outlook Express non blocca *tutti* gli allegati, ma soltanto quelli che Microsoft ritiene siano "potenzialmente pericolosi", non in base al loro contenuto specifico, ma quasi esclusivamente in base alla loro estensione.

Non è un criterio molto robusto: abbiamo già visto quanto sia facile ingannare Windows in fatto di estensioni. Inoltre **la lista di estensioni ritenute pericolose è incompleta:** non vengono bloccati, per esempio, i file con estensione *JPG* (immagini), che in alcune versioni non aggiornate di Windows possono trasportare virus, e i file con estensione *ZIP*, all'interno dei quali può essere annidato un virus.

La conseguenza di questa situazione infelice è che praticamente tutti gli utenti di Outlook Express disabilitano quest'opzione. Per poter ricevere gli allegati desiderati si sentono costretti a non bloccare nessun allegato, **compresi quelli sicuramente pericolosi.**

C'è però una soluzione meno drastica che consente di abilitare quest'opzione come **primo filtro antivirus** senza avere problemi con gli allegati desiderati: modificare la lista degli allegati che Windows ritiene pericolosi.[96]

In questo modo, gli allegati che assai probabilmente sono ostili (quelli con le estensioni *exe, com, scr, pif* e le altre citate nel Capitolo 3) vengono bloccati e non li potete aprire neppure se ci provate, ma gli allegati desiderati sono apribili, sia pure con la consueta cautela.

Ecco come procedere per effettuare questa modifica:

- in Outlook Express, assicuratevi di aver **attivato** l'opzione *"Non consentire salvataggio o apertura di allegati..."* citata sopra;

- avviate Esplora Risorse (lo so, sembra che non c'entri niente con gli allegati e con Outlook Express, ma fidatevi) e scegliete Strumenti > Opzioni cartella e la scheda *Tipi di file;*
- nell'elenco di estensioni che compare, trovate quella che vi interessa sbloccare (per esempio *DOC*) e cliccate su *Avanzate*, poi disattivate la casella *Conferma apertura dopo download*; dopo che avete cliccato su OK per chiudere le finestre di dialogo, tutti gli allegati con quell'estensione diventano apribili tramite Outlook Express.

Se l'estensione che vi interessa non è in elenco, quando arrivate all'elenco di estensioni, procedete come segue:

- cliccate su *Nuovo,* immettete (in maiuscolo o minuscolo) il nome dell'estensione desiderata nella casella *Estensione*, e cliccate su *Avanzate*;
- nel menu *Tipo file associato*, lasciate *<nuovo>* e cliccate su OK;
- a questo punto l'estensione desiderata compare nell'elenco e può essere impostata come descritto prima.

Se al contrario c'è un'estensione che Windows *non* ritiene pericolosa ma che volete bloccare, potete cercarla nell'elenco delle estensioni di Esplora Risorse e *attivare* la casella *Conferma apertura dopo download.*

> *Ricordate che **questo è soltanto un primo filtro** per debellare le principali estensioni ad alto rischio, e **non garantisce in alcun modo che i file che ricevete con estensioni non bloccate siano sicuri**. Restano valide le normali precauzioni: antivirus aggiornato e diffidenza generale verso ogni allegato.*

Ora che avete tolto di mezzo alcuni dei più brutti ceffi della Rete, resta da prendere una sana abitudine per quanto riguarda gli allegati che Outlook Express non blocca automaticamente: **non fare mai doppio clic su un allegato in Outlook Express**. Usate invece l'opzione *Salva allegati* del riquadro di anteprima oppure l'equivalente opzione *Salva con nome*, disponibile se fate doppio clic sul titolo di un messaggio.

In questo modo, l'allegato viene salvato sul vostro disco rigido *senza essere aperto* ed è quindi innocuo, a meno che siate così

imprudenti da cliccarvi sopra due volte. Potete esaminarlo a vostro piacimento con l'antivirus aggiornato e poi, se siete sicuri che si tratta di un allegato non infetto e che avete davvero bisogno di aprire, potete aprirlo usando il solito metodo *"apri con"*. Questa tecnica va adottata anche se usate un programma di posta alternativo a Outlook Express.

Igiene della posta in uscita

Se la posta HTML è male, è chiaro che oltre a non riceverla dovete anche evitare di inviarla. Per fortuna, questa è un'opzione molto semplice da attivare nel programma di posta Microsoft.

In Outlook Express, scegliete *Strumenti* > *Opzioni* e la scheda *Invio*. Disattivate la casella *Rispondi ai messaggi utilizzando il formato originale* e attivate *Testo normale* in *Formato invio posta*.

Fatto questo, se provate a comporre un messaggio, noterete che è scomparsa la possibilità di usare grassetti e corsivi e di inserire immagini. È il prezzo che si paga per regalare sicurezza alle persone alle quali mandate messaggi.

Niente ricevute ai pubblicitari

Questa non è una misura di sicurezza vera e propria: riguarda più che altro la vostra privacy. È un modo per tenere lontani gli *spammer*, i pubblicitari-spazzatura di Internet. Tuttavia, visto che spesso fra loro si annidano individui che non esitano a usare virus e altre tecniche da vandali per raggiungere i loro scopi, difendere la privacy contribuisce anche alla sicurezza.

Outlook Express ha un'opzione che manda automaticamente un messaggio che conferma al mittente che avete letto il suo e-mail: utile quando il mittente è una persona che conoscete, ma dannosissima se il mittente è un pubblicitario. Infatti il pubblicitario la sfrutta per sapere se il suo messaggio è stato letto e quindi il vostro indirizzo è ancora in uso: se riceve questa conferma, state sicuri che aumenterà il vostro bombardamento di posta-spazzatura.

Assicuratevi pertanto che in *Strumenti* > *Opzioni*, nella scheda *Conferme*, non sia attivata l'opzione *Invia sempre una conferma di lettura*. Scegliete una delle altre due: la prima non invia mai conferme a nessuno, mentre la seconda vi chiede ogni volta se volete inviarla.

Anteprime pericolose

La configurazione standard di Outlook Express divide la finestra del programma in tre parti: l'elenco delle cartelle di posta, l'elenco dei messaggi, e il *riquadro di anteprima.* Cliccando sul titolo di un messaggio, il testo di quel messaggio viene visualizzato automaticamente in questo riquadro di anteprima.

È un modo molto pratico e veloce di sfogliare i messaggi, ma comporta dei rischi per la sicurezza: con alcuni virus è sufficiente visualizzare un messaggio nell'anteprima e ci si ritrova infetti (non occorre aprire allegati).[97] Con le vecchie versioni di Outlook Express, un aggressore poteva addirittura usare l'anteprima per confezionare un messaggio che gli permetteva di leggere la vostra posta.[98]

Come se non bastasse, l'anteprima può facilmente sbattervi immagini pornografiche o comunque indesiderate sullo schermo: **le immagini allegate ai messaggi vengono infatti visualizzate automaticamente** non appena cliccate sul titolo di un e-mail, e non c'è modo di ordinare a Outlook Express di non mostrarle (salvo installare il Service Pack 2, con gli effetti descritti in dettaglio tra poco).

È insomma saggio **disattivare l'anteprima:** in Outlook Express, scegliete *Visualizza* > *Layout* e disattivate la casella *Visualizza riquadro di anteprima*. Sfogliare i messaggi richiederà qualche cliccata in più (anche se la barra di navigazione aiuta), ma è sempre meglio che infettarsi.

> *Se l'anteprima vi piace, tenete presente che esiste anche nei programmi di posta alternativi, ma senza i problemi di sicurezza che ha in Outlook Express.*

Cosa cambia con il Service Pack 2

Gli aggiornamenti del Service Pack 2 riguardanti la gestione della posta hanno effetto soltanto se usate Outlook Express. Se usate un programma alternativo, non noterete alcun cambiamento significativo.

Usando Outlook Express, invece, noterete delle novità importanti. Sono anni che si implora Microsoft di disattivare la visualizzazione della grafica nei messaggi in Outlook Express, in modo da evitargli

di visualizzare qualsiasi porcheria pornospammatoria gli venga mandata: un'opzione presente da tempo immemorabile in tutti gli altri programmi di posta. Finalmente le implorazioni hanno avuto effetto.[99]

Immagini al bando

Una volta installato il Service Pack 2, se avete scelto l'opzione *Leggi tutti i messaggi in testo normale*, finalmente Outlook Express non visualizza più automaticamente le immagini allegate ai messaggi. Per visualizzare le immagini presenti in un singolo messaggio, scegliete *Visualizza* > *Messaggio in HTML*.

Inoltre il menu Strumenti > Opzioni include, nella scheda Protezione, la nuova opzione *Blocca immagini e altri contenuti esterni nella posta elettronica HTML*. Questa è una funzione per contrastare i pubblicitari senza scrupoli, e vi consiglio di tenerla attivata.

Infatti attivando quest'opzione, se autorizzate un messaggio alla visualizzazione del suo contenuto HTML, come a volte è necessario fare quando ricevete un modulo o una comunicazione commerciale che vi interessa, verranno visualizzate soltanto le immagini *allegate* al messaggio. Eventuali immagini *esterne* (*linkate*, in gergo) verranno ignorate (Figura 12.5) e saranno visualizzate soltanto su vostra esplicita richiesta, per esempio scegliendo *Visualizza* > *Immagini bloccate*.

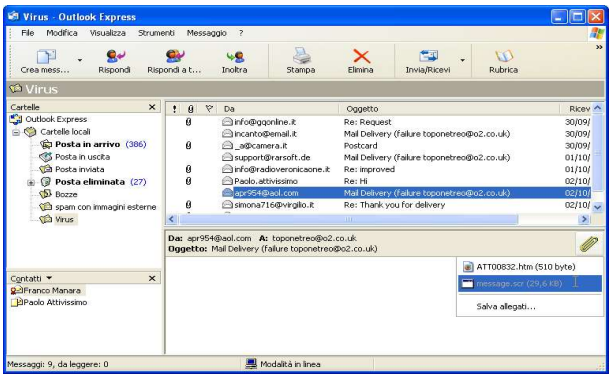

Figura 12.5

Gli *spammer* sfruttano queste immagini esterne, ossia non incluse nei messaggi ma residenti su Internet e collegate al messaggio tramite codici nascosti HTML, per sapere se leggete le pubblicità che vi mandano (ve lo dicevo, io, che l'HTML nella posta è male).

Come fanno? Infilano nei loro e-mail un collegamento o link a un'immagine che si trova sul loro sito. Di solito è un'immagine piccolissima e del medesimo colore dello sfondo, quindi invisibile a occhio nudo. Sono questi i *web bug* accennati nelle pagine precedenti.

Se aprite un messaggio confezionato in questo modo e avete impostato il vostro programma di posta in modo che visualizzi l'e-mail in HTML (anziché non in testo semplice come vi ho consigliato), Windows contatta automaticamente il sito dello *spammer* per scaricarne l'immagine collegata.

In questo modo lo *spammer* sa esattamente quanti utenti leggono i suoi messaggi; se oltretutto ha creato un'immagine collegata distinta per ciascun utente, sa anche *chi* ha letto i suoi messaggi e quindi quali indirizzi sono validi e pertanto ulteriormente bombardabili di spam. Brutto affare, vero?

Con il Service Pack 2, questo squallido espediente non funziona più se tenete attivata l'opzione *Blocca immagini e altri contenuti esterni nella posta elettronica HTML*.

Allegati meglio discriminati

Anche la gestione degli allegati di Outlook Express viene irrobustita: invece di dividere gli allegati semplicemente in buoni e cattivi, con il Service Pack 2 nasce la categoria degli allegati *sospetti*, che non vengono bloccati completamente ma sono accessibili soltanto dopo aver risposto a una finestra di dialogo di avvertimento (Figura 12.6).[100]

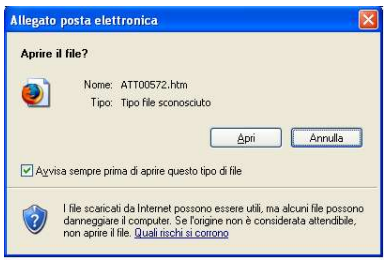

Figura 12.6

Se avete disattivato l'opzione Non consentire salvataggio o apertura di allegati che potrebbero contenere virus *(*Strumenti > Opzioni > Protezione*), tenete presente che viene riattivata automaticamente quando installate il Service Pack 2, che inoltre cambia l'elenco di estensioni proibite e aggiunge altri criteri di discriminazione oltre all'estensione.*[101]

Se non riuscite più ad aprire certi allegati desiderati dopo aver installato questo aggiornamento, controllate le impostazioni di quest'opzione.

*Fate attenzione inoltre a non cliccare con il pulsante **destro** sugli allegati in Outlook Express, perché in questo modo scavalcate la protezione del Service Pack 2.*

L'assegnazione dei file alle categorie "buoni", "cattivi" e "sospetti" non dipende più soltanto dalle loro estensioni, ma anche dalla loro *provenienza*: Windows, infatti, ora si ricorda se un file è stato scaricato da Internet o se proviene da altra fonte fidata (questa funzione richiede che usiate dischi formattati nel formato NTFS, che è quello solitamente usato da Windows XP).

Se salvate su disco un allegato, Windows lo può bloccare, sia pure in modo molto blando: il blocco si toglie cliccando sull'allegato con il pulsante destro in Esplora Risorse e scegliendo Proprietà e Annulla blocco. Tuttavia non c'è da fidarsi: molti allegati contenenti virus non vengono bloccati da questa funzione. Rimane valido il consiglio di esaminare **sempre** ogni allegato con un antivirus aggiornato.[102]

In sintesi, il Service Pack 2 pone rimedio ad alcune falle di sicurezza storiche di Outlook Express; tuttavia l'approccio scelto da Microsoft è piuttosto complicato da ricordare e non è a prova di bomba. È questione di gusti e di abitudini, ma probabilmente troverete più semplice l'approccio drastico dei programmi alternativi, che consentono già da tempo di non visualizzare le immagini e di salvare automaticamente tutti gli allegati senza aprirli, per poi sottoporli, comodamente ma senza eccezioni, al vaglio di un antivirus.

Capitolo 13

Trappole nella posta

Ora che la base tecnica della vostra gestione della posta è in ordine, vorrei proporvi alcuni consigli per difendersi dalle insidie non strettamente tecniche della posta elettronica. Molte delle principali trappole dell'e-mail si risolvono o diventano più facili da evitare grazie al lavoro di blindatura di Windows fatto nei capitoli precedenti, ma alcune sono indipendenti dallo strumento e mirano direttamente all'altro computer che avete in casa: il vostro cervello. In questo caso non c'è antivirus o firewall che tenga, e bisogna vaccinare la materia grigia.

Non temete: come vi diceva sempre il dottore durante le vaccinazioni vere, *"non farà male"*. Bugiardo schifoso. Spero di essere meno traditore.

Precauzioni di base

Comincerei, se permettete, con un breve ripasso delle cautele già viste:

> ***Mai, mai, mai dare in un e-mail numeri di carte di credito, password o altri dati personali segreti.*** *Se qualcuno ve li chiede, è un truffatore o un incosciente.*

Gli allegati sono il maggior pericolo per chi usa la posta:

> ***Regola 8: Non aprite gli allegati non attesi, di qualunque tipo, chiunque ne sia il mittente, e comunque non apriteli subito, anche se l'antivirus li dichiara "puliti".***

E a proposito di allegati e di chi ve li manda:

- **Non esistono tipi di file sicuri.** Forse lo è il testo semplice, ma è facile creare un file che *sembra* testo semplice.

- **È facilissimo falsificare il mittente di un e-mail**. Quindi non fidatevi se vi arriva una comunicazione di vincita a una lotteria o una richiesta di Microsoft di installare l'allegato aggiornamento.
- **È altrettanto facile creare file infetti non riconoscibili dagli antivirus**. Pertanto aprite gli allegati solo se strettamente necessario e se avete verificato l'autenticità della fonte.
- **Fra l'uscita di un nuovo virus e la disponibilità dell'antivirus aggiornato che lo riconosce passa del tempo**, durante il quale l'antivirus non blocca la nuova minaccia.
- **La posta HTML è male: la posta di testo semplice è bene.**

Phishing: la truffa arriva per posta

Regola 9. Non fidatevi dei link a banche o negozi forniti da sconosciuti. Possono essere falsi e portarvi a un sito-truffa. Usate invece i Preferiti o il copia-e-incolla, oppure digitateli a mano, in un browser sicuro.

Come accennato nel Capitolo 11, è facilissimo creare un e-mail che contiene un **link ingannevole**, che sembra rimandare a un sito regolare ma invece vi porta da tutt'altra parte, ossia a un sito visivamente identico a quello autentico ma in realtà gestito da truffatori. Questo sistema, denominato *phishing,* viene usato per commettere frodi, per esempio rubando password o codici di carta di credito, o per infettarvi, inducendovi con l'inganno a visitare un sito ostile.

L'attacco più comune avviene in questo modo: ricevete un e-mail in formato HTML che sembra provenire dal servizio clienti di qualche banca, provider o società di commercio elettronico. Il messaggio vi avvisa di un *"controllo a campione"* o di un *"problema di verifica dei dati"* e vi chiede di visitare il suo sito usando il link cortesemente fornito nell'e-mail.

Un ottimo esempio di truffa via Internet basata sull'uso di HTML, anteprima e grafica è fornito da Hutteman.com[103], dal quale è tratta la Figura 13.1. È un e-mail che ha tutta l'aria di provenire dal fa-

moso sito Paypal: un popolarissimo servizio di micropagamento, presso il quale gli utenti depositano somme di denaro reale per i loro acquisti online.

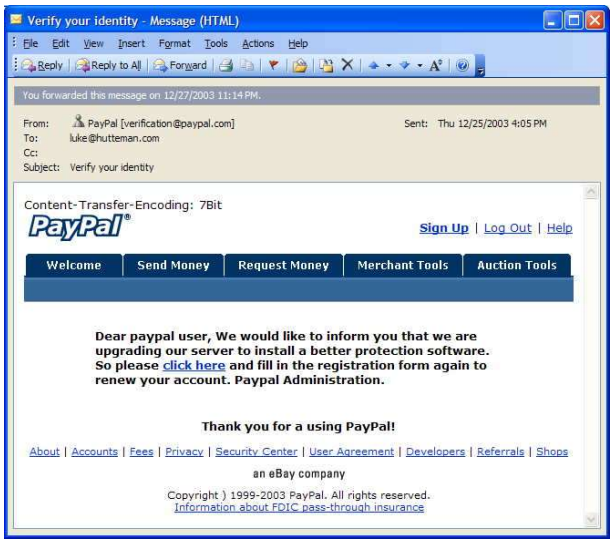

Figura 13.1

L'indirizzo del mittente, in questo esempio, è *verification@paypal.-com*; si vede il logo di Paypal; e soprattutto, il link *"click here",* sul quale il messaggio invita appunto a cliccare per *"reimmettere i propri dati di registrazione"*, rimanda al sito di Paypal. Non c'è nulla che induca al sospetto.

In realtà il mittente è falsificato e il messaggio è una truffa in piena regola ai danni dei correntisti Paypal (come il sottoscritto). Se vi fidate del messaggio e cliccate sul suo link *"click here"*, scatta la trappola informatica: il link infatti *sembra* portare a Paypal.com, ma in realtà porta a un sito-truffa che imita in tutto e per tutto il sito autentico.[104]

L'illusione di trovarsi nel sito vero è praticamente perfetta, ed è ovvio che gli utenti non sospettosi cadono nella trappola e regalano i propri dati personali (password compresa) al truffatore, che potrà così prosciugare il loro conto Paypal. Lo stesso meccanismo potrebbe essere usato con il sito della vostra banca.

Per evitare truffe di questo tipo occorre mantenere sempre alta la guardia e dubitare sempre dei link contenuti all'interno dei messaggi. Un altro espediente molto efficace per smascherare i tentativi di *phishing* è disattivare la visualizzazione dell'HTML: questo non solo elimina la forte "autenticazione" visiva data dalla grafica, ma rivela spesso la vera destinazione dei link.

Le Figure 13.2 e 13.3, per esempio, mostrano lo stesso messaggio-truffa, visualizzato con e senza HTML. Notate che la versione senza HTML indica il vero indirizzo al quale punta il link: è composto da numeri invece che da un nome, e questo è un chiaro campanello d'allarme, come accennato nel Capitolo 11.

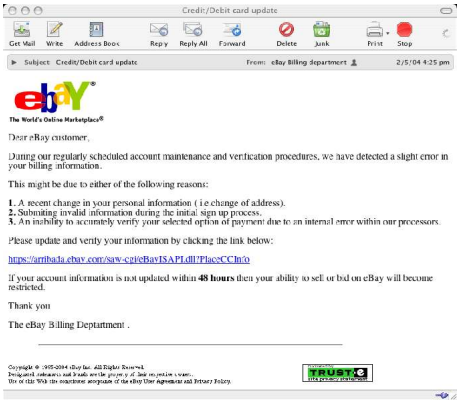

Figura 13.2

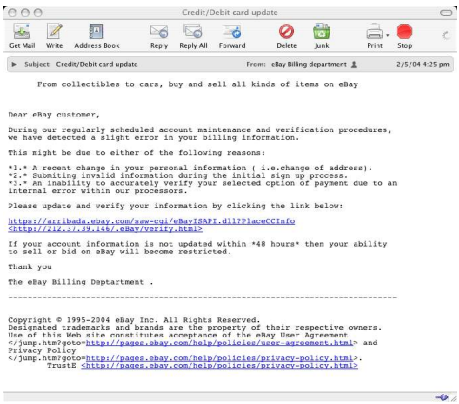

Figura 13.3

Il problema dei link fasulli si pone, sia pure in misura minore, anche con l'e-mail di testo semplice. Infatti è possibile confezionare un link che sembra portare a un sito ma in realtà porta altrove anche senza ricorrere all'HTML:

www.microsoft.com&item=q209354@3522684105

Ha tutta l'aria di portare al sito di Microsoft, ma in realtà porta a *www.playboy.com*. I browser moderni e sicuri, tuttavia, vi avviseranno del possibile pericolo o bloccheranno direttamente questo link. Se il vostro browser non lo fa, è il caso di cambiarlo.

Ricordate i tipici sintomi di un link fraudolento: chiocciolline e simboli di percentuale.

Spam: spazzatura digitale

Tutti abbiamo ricevuto nell'e-mail pubblicità indesiderate dei prodotti più disparati (e spesso anche piuttosto discutibili). È lo *spam*: la posta pubblicitaria-spazzatura che appesta Internet. Si stima che ormai oltre la metà dei messaggi in circolazione sia costituita da spam.

Cos'è veramente lo spam

Lo spam non è semplicemente una scocciatura che si elimina cancellandolo.

- **Porta pornografia in casa e in ufficio.** Lo spam arriva indiscriminatamente ad adulti e minori e spesso reclamizza pornografia, Viagra e altri coadiuvanti sessuali (presunti o reali), includendo immagini eloquenti.
- **Veicola truffe e virus.** Gli *spammer* sono venditori senza scrupoli: lo dimostra la loro stessa tecnica pubblicitaria, insensibile al buon gusto, alle regole della rete e alla privacy. Figuriamoci se gente di questa risma si prende la briga di essere onesta o di vendervi prodotti affidabili.
- **Intasa la Rete.** Gli spammer mandano *miliardi* di questi messaggi ogni giorno, per cui contribuiscono massicciamente a rallentare il traffico di messaggi della Rete. I loro messaggi, fra l'altro, sono spesso conditi di immagini e animazioni che li rendono ancora più pesanti.

- **Costa a *chi lo riceve*, cioè noi utenti**, a differenza della posta-spazzatura cartacea (che è pagata dal mittente). Lo paghiamo sotto forma di bollette telefoniche e di tempo perso ad aspettare che finisca lo scaricamento della posta e ad esaminare e cancellare le pubblicità indesiderate.

Come fa uno spammer ad avere il vostro indirizzo?

Gli spammer non sono dilettanti: sono organizzatissimi e sfruttano tutte le nuove tecnologie in una continua ricerca di modi per eludere le difese antispam che vengono man mano approntate.

- **Esplora automaticamente le pagine Web, i forum e i newsgroup con programmi automatici** che ne estraggono qualsiasi cosa che somigli a un indirizzo di e-mail.
- **Compra gli indirizzi da altri spammer.** Lo *spammer* ha sempre fame di nuovi indirizzi da bombardare. E chi, meglio di un altro *spammer*, può fornirglieli, naturalmente a pagamento?
- **Sfrutta le catene di sant'Antonio.** Questi messaggi contengono spesso centinaia di indirizzi di utenti che incautamente li hanno inoltrati senza occultare l'indirizzo del destinatario.
- **Crea siti Web che "catturano" il vostro indirizzo di e-mail quando li visitate.** Se immettete il vostro indirizzo di e-mail nei parametri di configurazione del vostro browser, è facile per uno *spammer* creare un sito Web che è in grado di indurre il browser a rivelarglielo.
- **Crea siti Web che invitano a lasciare il proprio indirizzo di e-mail per ricevere fantomatiche password di accesso** a immagini o filmati porno, musica da scaricare, programmi piratati e altre lusinghe. In realtà il sito non fa altro che accogliere con gioia il vostro indirizzo, magari dandovi un contentino per non farvi insospettire (e indurvi a segnalarlo ai vostri amici, che diverranno le prossime vittime).
- **Usa generatori random,** ossia programmi che generano automaticamente tutti i possibili indirizzi di e-mail di un fornitore d'accesso (per esempio da *aaaaaa@tin.it* a *zzzzzz@tin.it).*

Difese antispam

Il consiglio fondamentale è la prevenzione. Una volta che il vostro indirizzo arriva nelle grinfie degli spammer, siete praticamente spacciati. Certo, ci sono dei palliativi da adottare se sciaguratamente venite pescati da uno spammer, ma la loro efficacia è limitata.

- **Nessun indirizzo in chiaro nel vostro sito.** Anche per chi vuole farsi contattare via e-mail, indicare un indirizzo nel proprio sito non è indispensabile. Esiste, infatti, una tecnica elegante che permette di ricevere posta da sconosciuti senza rivelare il proprio indirizzo: è l'uso di un cosiddetto *form,* cioè di una pagina Web in cui si predispone uno spazio in cui l'utente può scrivere il proprio messaggio. Il messaggio viene poi inoltrato al vostro indirizzo di posta, che pertanto rimane segreto.
- **Se proprio dovete mettere il vostro indirizzo in una pagina Web, metterlo sotto forma di immagine grafica o mascheratelo.** In questo modo i programmi automatici degli spammer non riusciranno ad interpretarlo e sarete al sicuro dalle loro grinfie. L'unico difetto di questa tecnica è che penalizza i non vedenti, che non riusciranno a "leggere" l'indirizzo, per cui usatela soltanto nei casi più disperati.
  Un altro sistema che sembra reggere contro gli spammer e invece non ostacola i non vedenti è la conversione in simboli HTML. Daniele Raffo ha preparato una pagina Web (*www.crans.org/~raffo/aem*) che converte automaticamente l'indirizzo di e-mail che vi immettete.
- **Anonimizzate forum e newsgroup.** Molti utenti non sanno che non è assolutamente necessario specificare il proprio indirizzo di e-mail nei messaggi nei forum, nelle aree di chat o newsgroup: gli altri partecipanti non ne hanno bisogno per rispondervi, a meno che non vogliate una risposta privata.

  Molti programmi per la frequentazione dei newsgroup immettono automaticamente il vostro indirizzo di posta nei messaggi, perché è presente nei loro parametri di configurazione. Assicuratevi che il vostro programma non si comporti in questo modo.

- **Non rispondete MAI allo spam**, né per protestare, né per saperne di più su un'offerta allettante, né per "dis-iscrivervi".

Sono i trucchi più classici degli *spammer:* farvi arrabbiare, mandarvi offerte-civetta o offrire false opzioni di "dis-iscrizione". A loro interessa che rispondiate, così confermate che il vostro indirizzo è valido e attivo e quindi bombardabile.

- **Date il vostro indirizzo a pochi ma buoni.** Ammettiamolo: siamo spesso troppo disinvolti nel dare in giro il nostro indirizzo di e-mail. Dovremmo invece considerarlo alla stregua del nostro numero di cellulare, sul quale vogliamo essere raggiunti solo ed esclusivamente da persone che non ne abuseranno.
  Se ormai il vostro indirizzo è conosciuto anche dai sassi, cambiate indirizzo e date quello nuovo soltanto a chi veramente ne ha bisogno, e date a queste persone l'esplicito ordine di non darlo a nessuno.
- **Non memorizzate l'indirizzo nel browser.** Molti browser prevedono un'opzione che permette di memorizzare i vostri dati personali, in modo da evitare di doverli digitare ogni volta che qualche sito ve li chiede. È una comodità che si paga: è facile per uno *spammer* creare un sito in grado di indurre il browser a rivelargli tutti questi dati.
- **Non date l'indirizzo ai siti che ve lo chiedono, se non hanno una reputazione cristallina.** Legge sulla privacy o meno, esiste tuttora un mercato fiorente di compravendita di indirizzi di e-mail. Siate pertanto estremamente cauti nel dare il vostro indirizzo di e-mail ai siti che ve lo chiedono: dateglielo soltanto se si tratta di siti di reputazione più che buona.
  Se possibile, comunque, vi conviene creare un indirizzo di e-mail supplementare "sacrificabile" da dare a questi siti: in questo modo, se sgarrano e vendono il vostro indirizzo a uno spammer, potrete semplicemente chiudere l'indirizzo sacrificabile. Ci sono molti siti che offrono questo tipo di indirizzi, come Spamhole.com e Yahoo (AddressGuard).
- **Scegliete un nome utente lungo almeno dieci caratteri.** Questo manda in crisi i generatori di indirizzi usati dagli spammer: tentare tutte le possibili combinazioni di dieci caratteri richiederebbe *centomila miliardi* di tentativi.
- **Usate e fate usare sempre la "copia carbone nascosta".** L'opzione *"copia carbone"* o *"CC"* manda lo stesso messaggio a più persone, ma mostra a ogni destinatario indirizzi di tutti gli altri. Già questa è una scortesia, ma la cosa peggiore è che

molti usano la copia carbone anche per le catene di sant'Antonio, con il risultato che certi appelli viaggiano accompagnati da *centinaia* di indirizzi, pronti per essere intercettati da uno spammer (o da un virus).
Esiste però una variante della "copia carbone", che si chiama *"copia carbone nascosta"* (*CCN*) o *BCC* (dalle iniziali dell'equivalente inglese *blind carbon copy*) e nasconde a ciascun destinatario gli indirizzi degli altri. Purtroppo in alcuni programmi (Outlook Express, per esempio) questa variante è stata nascosta, e così pochi ne sono a conoscenza. Imparate ad usarla e fatela usare a chi conosce il vostro indirizzo di e-mail: in questo modo ne limiterete la diffusione.

> *In Outlook Express, l'opzione BCC si rende visibile componendo un messaggio e scegliendo* Visualizza > Tutte le intestazioni. *Basta farlo una volta sola e Outlook se ne ricorderà permanentemente.*

- **Vietate al vostro programma di posta di visualizzare automaticamente le immagini allegate ai messaggi.** Se uno spammer vi manda un'immagine porno, non ve la troverete subito sullo schermo appena aprite la posta.
- **Usate filtri antispam centralizzati.** Molti fornitori d'accesso offrono, con un leggero sovrapprezzo, caselle di posta sulle quali vigila un filtro antispam. Sono soldi ben spesi. Infatti questi filtri, inizialmente rudimentali, hanno oggi raggiunto un livello di sofisticazione davvero notevole: non sbagliano quasi mai, anche perché lasciano passare qualche messaggio di spam in più, piuttosto che bloccare erroneamente qualche e-mail legittimo.

Tecniche sostanzialmente inutili

- **Usare filtri antispam locali.** Alcuni programmi di posta dispongono di filtri antispam, che hanno un'efficacia molto elevata ma hanno il limite di dover essere personalizzati da ciascun utente e di agire soltanto *dopo* lo scaricamento individuale della posta, senza quindi risolvere il problema del costo di scaricamento dello spam. Se usati in combinazione con un filtro centralizzato, però, sono utili per cancellare automaticamente i pochi messaggi di spam che superano il filtro centralizzato.

- **Alterare il proprio indirizzo inserendo *ANTISPAM* e simili.** Molti utenti pensano di scansare lo spam alterando in un modo concordato il proprio indirizzo quando lo specificano nelle pagine Web e negli altri posti dove uno spammer può catturarlo. Per esempio, *topone@pobox.com* diventa *toponeANTISPAM@pobox.com,* oppure si sostituisce la chiocciolina con *"at"* (come in *topone(at)pobox.com*) e così via.
  Il problema è che gli spammer affinano ogni giorno le proprie armi, per cui tutti questi camuffamenti hanno vita breve e rendono difficile la vita ai principianti di Internet, che non sanno cosa significa *"at"* oppure non si rendono conto che "*antispam"* va rimosso dall'indirizzo prima di usarlo.
- **Presentare denunce al Garante della privacy.** È vero che il Garante è riuscito a risolvere qualche caso di spam, con tanto di indennizzo alle vittime,[105] ma gli spammer sono tanti, sono bersagli mobili e quasi sempre operano fuori dall'Italia, per cui sono al di fuori della portata delle leggi nazionali. Questa tecnica è utilizzabile soltanto per i pochi spammer italiani.
- **Denunciare il caso al vostro fornitore d'accesso.** Le società che forniscono accesso a Internet raramente puniscono i propri abbonati che fanno spamming, un po' per indolenza e un po' per necessità: gli spammer sono troppi, e se l'abbonamento di uno spammer viene chiuso, lo spammer non fa altro che aprirne uno nuovo.
- **Usare "liste bianche" o "liste nere".** Le "liste bianche" (o *whitelist*) sono elenchi personalizzati che specificano gli unici indirizzi che autorizzate a mandarvi e-mail. I messaggi provenienti da chiunque altro vengono respinti o semplicemente cancellati. Hanno un difettuccio: eliminano anche i messaggi legittimi degli utenti (nuovi amici o clienti, per esempio) che vogliono contattarvi.
  La "lista nera" (o *blacklist*) è una lista di indirizzi dai quali non desiderate ricevere posta. Quando ricevete uno spam, includete l'indirizzo dello spammer nella vostra *blacklist*, così non riceverete più posta dal malandrino. Ma gli spammer non usano quasi mai lo stesso indirizzo di posta, e spesso l'indirizzo indicato dagli spammer è completamente fasullo, per cui la vostra *blacklist* si riempie di indirizzi inutili.

- **Tentare di risalire al mittente.** Il mittente nei messaggi di spam è quasi sempre fasullo. Quand'anche fosse autentico, scoprireste che si trova quasi sempre al di fuori della giurisdizione della legge locale. Se però lo spam pubblicizza una società italiana, le possibilità di risalire al mittente e mandargli una multa inflitta dal Garante sono molto buone.
- **Mandare messaggi che sembrano indicare che il vostro indirizzo è inesistente.** Alcuni programmi di posta permettono di rispondere agli spammer mandando loro messaggi confezionati in modo da somigliare ai messaggi d'errore che si ottengono quando si scrive a un indirizzo inesistente. L'idea dietro questa tecnica è che se lo spammer si rende conto che quell'indirizzo è inesistente, smetterà di usarlo, ma gli spammer non fanno questo lavoro di fino. A loro non costa nulla mandare un milione di messaggi in più o in meno, per cui non perdono tempo a togliere dai propri elenchi gli indirizzi che non rispondono.

I trucchi della mente

"Se pensate che basti la tecnologia per risolvere i vostri problemi di sicurezza, non capite quali sono i problemi e non conoscete la tecnologia"

Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000)

È comodo affidarsi alla tecnologia e pensare di essere al sicuro perché si è comprata l'ultima diavoleria del settore. È facile trovarsi appisolati al volante del PC quando arrivano decine di messaggi. Ma se tenete sveglio e allenato il cervello, scoprirete che è un potentissimo antivirus. L'importante è capire quali sono i trucchi usati dagli aggressori per indurci ad abbassare le difese.

- Per esempio, c'è un modo molto semplice per capire se un e-mail ci arriva davvero da un conoscente o se il mittente è stato falsificato da un virus: un messaggio autentico userà un titolo pertinente, mentre un e-mail di origine virale dovrà restare vago, usando titoli come *"una foto per te"* o *"leggi questo".*
- Se un e-mail che afferma di provenire dalla vostra banca vi chiama *"egregio correntista"* invece di indicarvi con nome e cognome, è assai probabile che sia un tentativo di truffa.

- Se un'offerta che trovate in Rete vi sembra troppo bella per essere vera, è perché non è vera. Classico esempio: le offerte dei siti porno di chiedervi *"un solo dollaro di addebito sulla carta di credito"*. Come no: una volta che hanno il vostro numero, vi mungeranno.

Soltanto le capacità del cervello umano sono in grado di distinguere un caso dall'altro. È per questo che la tecnologia non basta.

Le tecniche di persuasione adottate da aggressori e truffatori vanno sotto il nome di *social engineering*, che si traduce liberamente con *fregare il prossimo con la psicologia.* Conoscere le tecniche di *social engineering* è il modo migliore per non finirne vittima.

> ***Non cominciate a dire "io sono troppo colto/intelligente per abboccare"**. Essere vittima del social engineering non è una questione di lauree o di quoziente intellettivo. Ho in archivio casi spettacolari riguardanti professionisti, professori, ingegneri e primari d'ospedale. Questi trucchi fanno leva su meccanismi istintivi, che non si cancellano certo con un titolo di studio.*

Le tecniche di base

Nell'arsenale psicologico dell'aggressore ci sono vari grimaldelli per scardinare le vostre difese mentali, da usare singolarmente o in combinazione per ottenere il risultato desiderato.

Come i trucchi dei prestigiatori, questi metodi perdono ogni mistero ed efficacia una volta svelati. Leggete queste brevi descrizioni e sarete vaccinati contro buona parte delle forme di aggressione psicologica della Rete.

- **Autorevolezza**. C'è qualcosa nell'e-mail che ci induce a **credere istintivamente alla sua autenticità.** Probabilmente è il fatto che l'e-mail, essendo visualizzata con caratteri tipografici, eredita l'autorevolezza della carta stampata o delle comunicazioni burocratiche ufficiali. Se non disattivate la grafica, un e-mail può anche contenere un logo aziendale o un altro marchio di fiducia, che ne aumenta ulteriormente l'autorevolezza (reale o apparente). Inoltre siamo tutti un po' condizionati ad accettare l'autorità altrui e a ubbidire ai comandi se impartiti con autorevolezza.
  L'aggressore fa leva sul cosiddetto **principio d'autorità**: si

spaccia per una fonte autorevole (un'azienda, un ente, un governo) e ci manda un messaggio in cui ci chiede per esempio di installare subito il software allegato (per esempio un falso "aggiornamento di sicurezza" di Windows) oppure di leggere il documento allegato o visitare un certo sito-trappola, oppure di mandargli le nostre password "per un controllo". L'allegato o il sito contengono software che veicola l'infezione o ruba i codici di accesso.

- **Colpa.** Tutti ci sentiamo colpevoli di qualche cosa, e probabilmente lo siamo. Non ditemi che non avete mai visitato un sito porno o usato software pirata o scaricato una canzone o un film da Internet. L'aggressore fa leva su questo **principio di colpa** per piegarvi al suo volere: vi fa credere di essere a conoscenza di un vostro misfatto e vi offre un modo per nasconderlo. In questo modo crea una complicità, si presenta come vostro salvatore, e voi cadete nella trappola di ubbidire ai suoi comandi.
  Per esempio, potreste ricevere un e-mail in cui un *"Ente di Sorveglianza Internet"* vi dice di essere al corrente di una vostra attività online illecita e vi propone di regolarizzare la vostra posizione installando il programma allegato all'e-mail. Sappiamo tutti che non si devono eseguire allegati di fonte sconosciuta, ma il senso di colpa tenderà a farcelo dimenticare. Naturalmente il programma allegato sarà un virus o simile.

- **Panico.** Un altro degli strumenti preferiti degli aggressori è **suscitare il panico**. Quando siamo spaventati, le nostre facoltà razionali si annebbiano e diventa più facile ingannarci.
  L'aggressore può, per esempio, inviarci un e-mail in cui dice che è in circolazione un pericolosissimo virus che non viene ancora rilevato dai normali antivirus, ma che viene debellato dal programma allegato; però bisogna fare presto!
  Ancora una volta, se la richiesta di eseguire l'allegato giungesse in un messaggio normale, non abboccheremmo: ma siccome siamo spaventati dal contenuto del messaggio, tendiamo a cadere nella trappola.

- **Ignoranza.** Ammettiamolo, è praticamente impossibile sapere tutto del funzionamento di Internet e di tutti i complicatissimi apparecchi che ci circondano. Così l'aggressore può confezionare un messaggio che sembra serio e affidabile perché usa

un sacco di paroloni tecnici che non capiamo ma che (nella nostra ignoranza) ci sembrano plausibili.

- **Desiderio.** Certi istinti primordiali sono una manna dal cielo per chi vuol fregarvi. Per esempio, l'idea di poter scaricare immagini e filmati porno manda in pappa il cervello di quasi tutti gli utenti maschi. Se un maschietto riceve un e-mail che gli promette formose visioni (magari di qualche personaggio famoso) se solo esegue l'allegato programmino o visita un certo sito, state certi che abboccherà quasi sempre, anche se in circostanze normali sarebbe stato più guardingo. Il sesso è una molla classica degli inganni online: gli anni passano, ma funziona sempre.
- **Avidità.** Anche l'avidità è uno strumento prezioso per l'aggressore. È difficile resistere al richiamo di chi sembra offrirci un "affare eccezionale" o un "sistema infallibile" per diventare ricchi o piratare il software o avere qualcosa a scrocco (musica, suonerie per cellulari, vincite alla lotteria). Purtroppo si tende sempre a dimenticare che nessuno dà niente per niente.
- **Buoni sentimenti.** La pornografia è il grimaldello ideale per far vittime fra i maschi, ma con il gentil sesso non attacca. Ci vuole un approccio più sofisticato, più *soft*. In questo caso gli aggressori usano sedurre le proprie vittime ricorrendo a espedienti che fanno leva sull'amore o sui buoni sentimenti (meglio se un po' sdolcinati).
  Per esempio, l'aggressore invia un e-mail in cui dice che *"qualcuno ti sta pensando, se vuoi sapere chi è, clicca sull'allegato"*. Uno dei virus più devastanti si chiamava *I love you* dal titolo del messaggio che lo accompagnava: quest'anonima dichiarazione d'amore fu sufficiente a indurre milioni di utenti (maschi e femmine) ad aprire l'allegato, attratti dall'esplicita lusinga, facendosi sistematicamente infettare.
  Un altro esempio di questa tecnica è dato dai tanti e-mail che contengono strazianti appelli per salvare bambini malati o nidiate di gattini o per fare donazioni a favore di enti più o meno sconosciuti: sono quasi sempre trucchi per indurvi a comunicare i dati della vostra carta di credito o a visitare un sito che tenterà di infettarvi. Gli enti benefici veri, quelli legittimi, difficilmente distribuiscono appelli via e-mail.

Come difendersi

Ora che conoscete per sommi capi le tecniche di social engineering, **siete già in gran parte vaccinati**. Quando ricevete un messaggio che sembra far leva su questi trucchi psicologici e vi chiede di fare qualcosa, verificatelo prima di decidere cosa farne. Chiamate un vostro amico o collega, oppure informatevi in giro tramite Google sull'esistenza di un eventuale comunicato ufficiale che confermi l'autenticità del messaggio. **Nel dubbio, non fate nulla** e soprattutto **non eseguite le istruzioni ricevute.**

Ovviamente non occorre arrivare alla paranoia costante. Tutto dipende dall'importanza del messaggio. Se si tratta della vostra banca (o di qualcuno che si spaccia per essa), è meglio alzare la guardia; se si tratta di chiacchiere innocue fra amici, è esagerato verificare rigorosamente l'autenticità di ogni singolo messaggio. Di solito è sufficiente riflettere un momento sul contesto.

La tecnica nigeriana e le vincite alla lotteria

La fantasia dei truffatori è fertilissima, e non è possibile catalogare qui tutte le infinite varianti partorite da questi artisti del raggiro. Ce ne sono un paio, tuttavia, la cui diffusione capillare merita una segnalazione particolare.

La prima è la cosiddetta *truffa alla nigeriana* (il nome deriva dal paese dove questo genere di raggiro ha raggiunto proporzioni industriali). Ricevete un e-mail, a volte in inglese ma sempre più spesso in un italiano un po' maccheronico, da parte di qualcuno che si presenta come un importante funzionario o notaio di un paese africano. Costui ha deciso di contattare voi, ma proprio voi, su consiglio di un imprecisato "comune conoscente", per chiedervi di fare da prestanome per riscuotere un'ingente somma di denaro, di provenienza non proprio cristallina, offrendovi in cambio una congrua percentuale.

Non ci vuole un intelletto da Einstein per intuire che c'è qualcosa che non quadra. Questo non impedisce a questa truffa, e alle sue varianti con persone malate che decidono di redimersi in punto di morte e vi vogliono regalare denaro, mogli di dittatori dissoluti che cercano un amministratore per restituire il maltolto alla popolazione, astronauti bloccati in orbita dal congelamento dei fondi per il rientro e quant'altro, di mietere vittime, mungendo loro soldi. Il bello è che *funziona*. Secondo le poste statunitensi, l'ammontare del

raggiro è di circa 100 milioni di dollari l'anno soltanto verso gli Stati Uniti. L'avidità è uno dei grimaldelli più efficaci.

Quello che invece non è evidente a molti è il meccanismo della truffa. Se rispondete a uno di questi appelli, prima o poi vi verranno chiesti dei soldi per "formalità burocratiche" o per "ungere un funzionario corrotto". Se siete così sconsiderati da mandarli, dopo un po' salterà fuori che c'è qualche altro "piccolo problema" che richiede un'altra somma, e così via. Vi manderanno anche dei documenti che "provano" l'iter burocratico in corso. I documenti sono ovviamente falsi, e dei milioni di dollari promessi non vedrete mai nemmeno l'ombra.

La seconda truffa onnipresente è la falsa vincita alla lotteria. Ricevete un e-mail da una fantomatica società di gestione di una lotteria estera, che vi comunica che siete stati estratti e avete vinto un premio in denaro. Presentando i codici di riferimento indicati nel messaggio, potrete riscuotere la vostra vincita.

Il meccanismo truffaldino è simile a quello della truffa alla nigeriana: per mettere le mani sul premio, dovreste versare un "piccolo contributo spese". Se abboccate, verranno addotti pretesti sempre nuovi per farvi mandare altro denaro agli organizzatori della truffa. La vincita, ovviamente, non vi arriverà mai.

Al lupo, al lupo: allarmi nella stampa e nella posta

Regola 12: Non fidatevi dei messaggi di allarme diffusi da stampa generalista, amici e colleghi, e non diffondeteli, se non sono documentati.

La Rete e i giornali non specialistici sono pieni di falsi allarmi riguardanti virus inesistenti o la cui azione è descritta con tragica incompetenza. Gli utenti ingenui diffondono questi allarmi ad amici e colleghi credendo di aiutarli. In realtà avvisi di questo genere non servono a nulla, se non a generare insicurezza e traffico inutile di messaggi.

- Fidatevi soltanto delle informazioni pubblicate dai siti antivirus o dagli addetti ai lavori.
- Diffidate degli avvisi pubblicati dai giornalisti non specializzati.

- Nel dubbio, non inoltrate nulla. Non cadete nella diffusa trappola del *"non so se è vero, ma nel dubbio lo inoltro"*. Il rischio di fare disinformazione è altissimo.

Se ricevete un allarme che vi lascia perplessi, controllate i siti antivirus e antibufala prima di decidere che fare: molto spesso è sufficiente immettere le parole-chiave dell'appello in Google. Se scoprite che qualcuno vi ha mandato un avviso fasullo, scrivetegli informandolo del suo errore e indicando la fonte della smentita, in modo da stroncare la diffusione del falso allarme.

Il modo migliore per distinguere un vero allarme di sicurezza da uno falso è vedere se include un rimando a un sito di un produttore di antivirus. Se il rimando è autentico e descrive quanto indicato nell'allarme, allora l'allarme è reale. Altrimenti, anche se ve lo manda il vostro migliore amico o lo dice la TV o il giornale, è meglio diffidare e non diffondere ulteriormente (e magari mandare due righe al vostro amico o al giornalista per avvisarlo che ha preso un granchio).

Niente catene di sant'Antonio!

Le *catene di sant'Antonio* sono parenti stretti degli allarmi che circolano tramite e-mail. Di solito non hanno un contenuto allarmistico vero e proprio, ma contengono frasette filosofiche o portafortuna che se non vengono inoltrate a tutti coloro che conoscete vi porteranno una iella cosmica.

Non inoltratele. Chi usa Internet da un po' di tempo ha già visto e subito tutte le catene di sant'Antonio possibili e immaginabili e non ne può più. Non funzionano neppure come rimedi antisfiga: io non le inoltro mai a nessuno, e l'unico risultato di tutte le maledizioni che avrei accumulato è un lieve accrescimento dei peli nel naso, e anche su quello ho qualche dubbio che sia colpa delle catene di sant'Antonio.

Un'altra ragione importante per non inoltrarle è che sono la gioia degli spammer e dei virus. Molti utenti, infatti, le inoltrano usando l'opzione *CC* descritta prima, per cui queste catene viaggiano accompagnate da *centinaia* di indirizzi, che gli spammer raccolgono e usano per indirizzare i loro messaggi pubblicitari e che i virus leggono dal vostro disco rigido per sceglierli come prossime vittime.

***Non diffondete mai un appello dal posto di lavoro**, altrimenti date l'impressione che l'azienda o l'istituto presso il quale lavorate ne confermino l'autenticità con la "firma" che viene spesso aggiunta automaticamente in calce agli e-mail aziendali. Molte persone sono state danneggiate da questo loro comportamento incauto: cercate di non ripetere i loro errori.*

Bufale

Un altro tipo di piaga dell'e-mail che si basa sulla psicologia è la bufala. Su Internet circolano appelli di ogni sorta: allarmi per la deforestazione, richieste d'aiuto per fermare i pazzi che allevano i gatti nelle bottiglie, bambini malati che vogliono entrare nel Guinness dei Primati con il maggior numero di cartoline di auguri, e le dicerie più strampalate, spesso a sfondo politico o razziale.

La stragrande maggioranza di questi allarmi è falsa o comunque disinformante. Sono pochissimi quelli autentici: per cui, a costo di sembrare cinici, è meglio partire dal presupposto che siano tutti falsi fino a prova contraria. Continuano a circolare, nonostante siano spesso evidentemente falsi, perché fanno leva sui pregiudizi, sulle paure nascoste, e sul principio d'autorità, perché ci arrivano sempre da persone che conosciamo e di cui ci fidiamo.

Per fortuna, grazie a Internet è abbastanza facile scoprire se un appello è autentico. Se ha avuto ampia diffusione, probabilmente è già stato analizzato da qualcuno dei tanti siti antibufala disponibili in Rete in varie lingue. Eccone alcuni.

- Centro per la Raccolta delle Voci e delle Leggende Contemporanee (*leggende.clab.it*, in italiano)
- *it.discussioni.leggende.metropolitane*, storico newsgroup italiano
- Urban Legends (*urbanlegends.miningco.com*, in inglese)
- Museum of Hoaxes (*www.museumofhoaxes.com*, in inglese)
- Vmyths (*www.vmyths.com*, in inglese, specializzato in bufale informatiche)
- Email Junkyard (*www.emailjunkyard.com*, in inglese)

- Hoaxbuster (*www.hoaxbuster.com*, in inglese e francese)
- Break the Chain (*www.breakthechain.org*, in inglese)

Anch'io, nel mio piccolo, ho raccolto una collezione di indagini anti-bufala presso *www.attivissimo.net/antibufala*.

Capitolo 14

Qualche altra falla da turare

Chat: caute chiacchiere al computer

Chat (*"chiacchiera"*, in inglese) è il termine usato per indicare lo scambio istantaneo di messaggi via Internet con parenti e amici vicini e lontani. Grazie a programmi gratuiti come *MSN Messenger, Yahoo Messenger, ICQ, mIRC* e tanti altri offerti da vari siti della Rete, non solo si può comunicare dietro l'angolo o su grandissime distanze senza svenarsi in telefonate, ma si possono anche scambiare fotografie e file di ogni genere; ci si può persino vedere in diretta, a mo' di videotelefono, se si collega al computer un'apposita telecamera (*webcam*), come mostrato nella Figura 14.1.

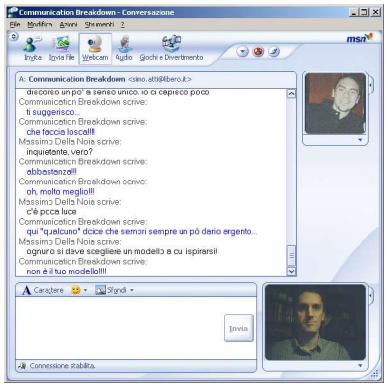

Figura 14.1

Chattare è molto divertente e coinvolgente, ma i programmi di chat si prestano anche a usi non troppo gradevoli. Le cronache dei giornali hanno fatto parecchio terrorismo sul tema, ma una volta tanto c'è un fondo di verità.

A differenza degli altri modi di interagire con Internet, infatti, la chat non comporta soltanto rischi di natura informatica. Se non prendete (e fate prendere) qualche semplice precauzione, rischiate di trovarvi in situazioni anche fisicamente spiacevoli, perché alcune

aree di chat sono frequentate da persone decisamente poco raccomandabili. È un problema che riguarda principalmente i minori, ma tocca anche il gentil sesso.

Non è il caso di criminalizzare la chat nel suo complesso, perché i suoi usi positivi sono di gran lunga superiori a quelli negativi. Basta capirne i meccanismi informatici e sociali e comportarsi di conseguenza.

Il concetto fondamentale da tenere presente è che **non c'è alcuna garanzia di identificazione: chiunque può spacciarsi per chiunque altro in una sessione di chat**. La chat "normale" (senza telecamera) non rivela sesso, età, tratti somatici, inflessione della voce. Potreste pensare di chattare con una brasiliana di Copacabana quando invece dall'altra parte della Rete c'è un idraulico sudaticcio in canottiera.

L'altro concetto fondamentale è che c'è una differenza enorme, in termini di sicurezza, fra chattare con persone che conoscete già bene nella vita reale e chattare con sconosciuti. La chat fra amici è un piacere che sarebbe sciocco guastare con paure inutili. **Chattare con i conoscenti non è pericoloso** (a parte qualche "normale" rischio informatico, come i virus e gli allegati infetti); **andare nelle aree di Internet dove si chatta fra sconosciuti lo è**.

Ecco quindi alcune raccomandazioni da seguire soprattutto se frequentate le *chat* anonime o se avete figli che lo fanno:

- **Non immettete i vostri dati personali nel "profilo utente" proposto da molti servizi di chat**. Se non impostate correttamente le opzioni di privacy, questi dati possono essere letti anche dagli sconosciuti.
- **Non usate il vostro nome e cognome: sostituiteli con un "nome di battaglia" *(nickname*)**, preferibilmente uno che non riveli di che sesso siete. Le donne sono facilmente oggetto di molestie.
- **Non usate il vostro indirizzo di e-mail come "nome di battaglia".** Questo evita che alcuni virus specializzati in chat riescano a rubare il vostro indirizzo e offre un appiglio in meno ai molestatori.
- **Non date mai i vostri dati personali a persone che conoscete soltanto via Internet.** Se ve li chiedono, siate molto sospettosi. Non occorre essere scortesi: basta restare nel vago,

indicando per esempio il capoluogo più vicino a voi. Di certo non è il caso di dare numeri di telefono o indirizzi di casa a persone che non conoscete. I codici delle carte di credito o le password, ovviamente, non vanno dati in chat neanche per sogno.

- **Siate molto cauti se qualcuno in chat mostra di sapere qualcosa di voi che non dovrebbe conoscere.** È facile "origliare" una conversazione tenuta via Internet ed estrarne informazioni da usare per sembrare "uno di famiglia" o un coetaneo.
- **Non commettete l'errore di pensare che siete adulti e quindi invulnerabili.** Alcuni molestatori usano la falsa intimità creata da questa forma di comunicazione per guadagnarsi gradatamente la vostra fiducia e poi vi devastano con attacchi verbali o minacce. C'è gente che non ha di meglio da fare, purtroppo, e Internet è per loro un terreno di gioco ideale.
- **Attenzione ai file ricevuti via chat**. Per questi file valgono le stesse precauzioni consigliate per i file allegati all'e-mail o scaricati durante le navigazioni nel Web: antivirus aggiornato e molta cautela. Anche le immagini possono essere un problema, se il loro contenuto è offensivo o pornografico.
- **Ricordatevi che siete voi ad avere la situazione in mano**. Siete al sicuro, a casa vostra: tutto quello che dovete fare per uscire da una conversazione imbarazzante è chiudere il programma. Il vostro interlocutore è anonimo, ma se siete stati prudenti, lo siete anche voi.
- **Se qualcuno dice qualcosa che non vi piace, fa domande troppo personali o vi mette a disagio**, "eliminatelo" chiudendo la sessione di chat e mettendo la sua utenza nella lista degli indesiderati (che verranno bloccati automaticamente) e parlatene con gli amici o con i genitori.
- **Non accettate mai un primo incontro faccia a faccia in un luogo privato.** Incontratevi in un luogo pubblico che vi è familiare e dove potete esaminare con discrezione l'interlocutore conosciuto in Rete prima di presentarvi. Portate con voi un amico o un'amica di cui vi fidate. Se vi accorgete che la persona è ben diversa da quello che diceva di essere in chat, scappate senza esitazione.

- **I *"groomer"***, ossia coloro che coltivano le proprie vittime adulte e minorenni, **sono persone molto intelligenti e non improvvisano.** Questi individui studiano la propria preda, ne imparano la cultura, il gergo e i gusti musicali e assumono in chat personalità adolescenziali per sembrare innocui.

Se ci riflettete un momento, noterete che queste sono raccomandazioni chiaramente derivate da quelle classiche che si fanno da sempre per evitare brutti incontri nella vita reale. Dovrebbero essere così ovvie da non essere necessarie, ma per motivi psicologicamente oscuri, **quando siamo in Rete tendiamo a fidarci molto di più degli interlocutori** che incontriamo nella nebbia dei bit di quanto faremmo in una situazione reale. È un comportamento istintivo che è necessario disimparare.

Trovate molte informazioni utili sul tema della lotta alle molestie e alla pedofilia online in Italia presso il sito della Polizia di Stato, all'indirizzo www.poliziadistato.it/pds/primapagina/pedofilia/index.-htm, e presso il Ministero dell'Interno (www.interno.it/sezioni/attivita/minori/s_000000200.htm).

P2P: scaricare musica con sicurezza

Sono moltissimi gli utenti che adoperano i cosiddetti programmi *peer-to-peer* o *P2P*, ossia programmi che consentono di condividere file musicali, video e immagini con gli altri utenti della Rete, con nomi come *Morpheus, WinMX, Kazaa* ed *eMule*. Purtroppo sono anche moltissimi gli utenti che li usano incautamente e si fanno quindi infettare o spiare tramite il computer.

Questa non è la sede adatta per una disquisizione sulla pirateria video e musicale perpetrata tramite i circuiti P2P. Vale però la pena di notare che usare questi circuiti di scambio non è di per sé illegale, come molte campagne (dis)informative tendono a far credere.

Se i diritti d'autore sui file scambiati ne consentono la libera distribuzione, scambiarli è perfettamente lecito. Per esempio, è legalissimo pubblicare un proprio video amatoriale su un circuito di scambio e lasciare che gli altri lo scarichino. Anche la versione elettronica di questo libro

può circolare sui circuiti di scambio: è una libertà prevista dalle sue condizioni di distribuzione.

Virus anche qui, dannazione

I circuiti di scambio di file non sono soggetti ad alcuna supervisione: sono scambi "fra pari" (è questo il significato dell'inglese *peer-to-peer*). In altre parole, chiunque vi può immettere qualunque tipo di file. E quel "qualunque tipo" include, inevitabilmente, anche i virus. Ci sono anche virus concepiti specificamente per diffondersi tramite questi circuiti.[106]

Di conseguenza, **qualsiasi file scaricato da un circuito P2P va controllato con l'antivirus aggiornato**, esattamente come se l'aveste ricevuto come allegato a un e-mail. La guardia non va abbassata neanche per i brani musicali e i filmati: anche questi file, infatti, possono contenere istruzioni ostili. Possono per esempio lanciare Internet Explorer per collegarsi a un sito contenente un virus e installarlo sul vostro PC.

Inoltre valgono anche qui tutti i trucchi basati sulle false estensioni dei nomi dei file descritti nei capitoli precedenti, per cui usate il vostro fedele *Apri con* invece della brutale doppia cliccata.

Non scaricate mai un programma da un circuito di scambio! *Se vedete in uno di questi circuiti un file il cui nome richiama quello di un programma molto diffuso e costoso, per esempio AutoCAD* o *Photoshop, i casi sono due: o è una copia pirata, con tutte le ovvie conseguenze in fatto di affidabilità e legalità, oppure è un virus il cui nome allettante è pensato per invogliarvi a scaricarlo. Non andate a cercarvi guai inutilmente.*

La breccia nei bastioni

Il problema di sicurezza fondamentale di tutti i programmi usati per partecipare ai circuiti di scambio è che **per loro natura devono permettere a chiunque di leggere e scaricare** (almeno parzialmente) **il contenuto del vostro computer**. Nel contempo, questi programmi devono **consentire a sconosciuti di scrivere file di origine ignota nel vostro PC**.

Non ci vuole una laurea in informatica per capire che questo scenario non è dei più tranquillizzanti. Equivale ad abbassare il ponte levatoio e far entrare chiunque nel proprio castello, sperando che si comporti bene e che bastino le poche guardie interne a tenerlo a bada. Ma se fate entrare così disinvoltamente dei potenziali aggressori, perché avete perso tempo a costruire i bastioni?

Usare un programma P2P significa creare una breccia che trapassa completamente tutte le vostre difese. L'unica cosa che impedisce agli aggressori di leggere i vostri file privati o di scrivere quello che vogliono nel vostro PC è il programma P2P. Se c'è una falla in quel programma, siete fritti. È quello che è successo per esempio con *Earth Station 5*, che si definiva *"il P2P più sicuro"*: in realtà consentiva a un aggressore di cancellare qualsiasi file sul computer dell'utente.[107]

C'è poi anche il rischio di un errore d'impostazione. Ogni programma di scambio file ha infatti un'opzione che definisce quali sono le *cartelle condivise*, ossia le cartelle del vostro computer che volete rendere accessibili a tutta Internet. Se sbagliate a definire queste cartelle e assegnate la condivisione per esempio all'intero disco rigido, **chiunque potrà leggere tutto quello che avete sul computer.** È un errore molto comune.

L'altro problema dei programmi di scambio è che molti di essi **contengono spyware**: è il caso (o lo è stato) di Kazaa, Limewire, Audiogalaxy, Bearshare, Imesh, Morpheus e Grokster, giusto per fare qualche nome.[108] Per sapere se un programma ospita spyware, vi conviene immettere in Google il nome del programma e la parola *spyware* e chiedere ad amici e colleghi che lo usano.

Per farla breve, se usate il computer per lavoro, non usate programmi di scambio. Prima o poi lo rimpiangereste. Tenete un computer separato per queste cose.

Psst... lo vuoi questo giochino?

Un altro rischio sicurezza molto frequente è dato dai programmi "prestati" da colleghi e amici. Si tratta spesso di copie pirata o di programmi di provenienza poco chiara, ma il problema riguarda anche i CD di programmi legalmente inclusi nelle riviste e persino nelle confezioni di cereali. Comunque sia, **cercate di farne a meno.**

Ci sono due ragioni fondamentali per questa raccomandazione. La prima è che molto software pirata è duplicato male, per cui non funziona (o funziona per un po' e poi si pianta, lasciandovi in braghe di tela), oppure è infetto da virus. Montereste sulla vostra auto pneumatici venduti da un tipo sospetto a un angolo di strada?

Inoltre la pirateria informatica è un concetto purtroppo ignorato con eccessiva disinvoltura. Esiste moltissimo software legalmente copiabile e distribuibile che fa le stesse cose di quello a pagamento: per esempio *Linux*, un sistema operativo completo che sostituisce Windows, e *OpenOffice.org*, alternativa gratuita a Microsoft Office. Di conseguenza, non c'è alcuna vera scusa che giustifichi la pirateria dei programmi.

La seconda ragione è un po' più tecnica. **Ogni volta che installate e disinstallate un programma, Windows tende ad accumulare "sporcizia"**: file superflui, file di sistema sostituiti con versioni diverse, voci del registro di configurazione, tipi di file riassegnati a un programma nuovo, e via dicendo.

Quando disinstallate un programma, in realtà non ne eliminate ogni traccia, e non riportate le cose a com'erano: Windows rimane sempre un po' cambiato.

A furia di fare installazioni e disinstallazioni, insomma, Windows perde stabilità e può modificare il proprio funzionamento in modi non sempre gradevoli. Più cose installate nel vostro computer, più vi esponete al rischio di cambiarne o appesantirne il funzionamento. Di conseguenza, è meglio evitare di installare del software "per prova", anche se di provenienza assolutamente non sospetta.

Se volete o dovete farlo, vi conviene creare preventivamente un backup immagine del disco rigido, installare il programma e poi ripristinare il computer al suo stato originale pre-installazione usando il backup.

Da tutte queste considerazioni nasce la Regola 5 del Dodecalogo:

> ***Regola 5: Non installate software superfluo o di dubbia provenienza.***

Per **dubbia provenienza** intendo anche siti che promettono di offrire suonerie, musica o pornografia gratis scaricando un *"programma gratuito"* che in realtà è un *dialer*. Scaricate programmi soltanto da siti di indubbia reputazione, come le biblioteche di soft-

ware di Internet. Per sapere se un sito ha una reputazione solida, chiedete ai vostri amici informatici.

Giù le mani dal mio piccì

La **sicurezza fisica** del computer, ossia la difesa contro gli aggressori e i pasticcioni che possono mettere le mani materialmente sul vostro PC, è una materia complessa, di cui teoricamente questo libriccino[109] non dovrebbe occuparsi.

Ci sono però un paio di cose relativamente semplici che potete fare per limitare l'accesso fisico al vostro computer: non impediranno ai malintenzionati esperti di portarvelo via o di carpirne i dati, ma terranno lontana gran parte dei[110] ficcanaso dilettanti e i colleghi e familiari con le mani di burro che tentassero di curiosare nel computer o modificarne maldestramente il funzionamento approfittando della vostra assenza.

> *Usate queste tecniche di difesa con cautela, altrimenti rischiate di non poter più accedere al vostro PC. Se non vi sentite tranquilli, fatevi guidare da un esperto.*

Apriti Sesamo: password di avvio

Non perdete tempo a impostare la password di avvio di Windows: esiste una miriade di modi per aggirarla. Per esempio:

- Basta infilare nel computer, durante l'avvio, un dischetto o un CD contenente un altro sistema operativo, che partirà al posto di Windows, dando accesso a tutti i dati presenti nel computer.
- In Windows XP Home esiste un utente "nascosto", denominato *Administrator*, che è *onnipotente e privo di password* (un classico esempio di progettazione intelligente). Per evocarlo, basta avviare il computer in modalità provvisoria, come descritto nel Capitolo 6, scegliere l'utente *Administrator* e premere Invio quando viene chiesta la password, ottenendo completo accesso ai dati.[111]
- Anche in Windows XP Professional esiste un utente di nome *guest* che spesso è accessibile all'avvio e consente un accesso limitato ma comunque sgradevole al computer.[112]

C'è un modo molto più robusto di proteggere il computer: la cosiddetta *password del BIOS*. Il BIOS è un chip, presente in tutti i computer, che contiene una sorta di mini-sistema operativo. È la prima cosa che parte quando accendete il computer, prima ancora di Windows o di qualsiasi altro sistema operativo su dischetto o CD.

Se mettete una password sull'accesso a questo BIOS, nessuno potrà avviare il vostro computer, salvo gli aggressori più esperti, che oltretutto avranno bisogno di molto tempo per agire. È l'equivalente informatico delle chiavi dell'auto.[113]

Per attivare questa protezione, spegnete e riaccendete il computer, dando un'occhiata agli strani messaggi di avvio (quelli che di solito ignorate). Dovrebbero includere una dicitura del tipo *Press DEL to enter Setup*, ossia "Premi il tasto Canc per accedere alla configurazione del BIOS". Se non trovate quest'indicazione, consultate il manuale del PC (non quello di Windows). Il tasto da premere può variare da computer a computer.

Pigiando questo tasto, interrompete il normale avvio del computer e vi trovate di fronte a una schermata simile a quella mostrata nella Figura 14.2.

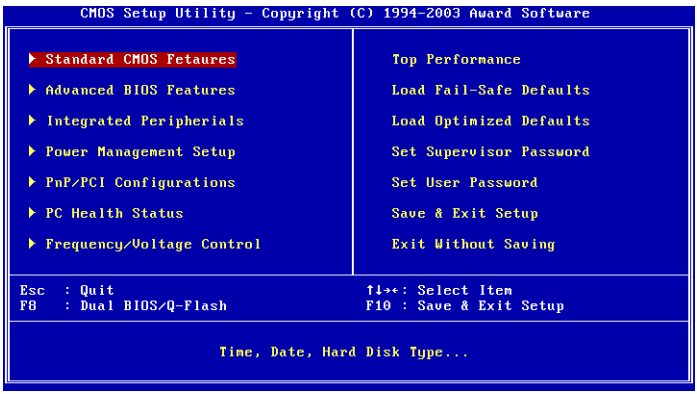

Figura 14.2

A questo punto, scegliete tramite i tasti freccia l'opzione che parla di *Password*: se ce n'è più d'una, scegliete prima quella riferita al supervisore (*Supervisor*), premete Invio e immettete una password di vostro gradimento.[114]

La password va immessa due volte, per evitare errori di battitura, e non viene visualizzata, per evitare che qualcuno la sbirci.

> *Assicuratevi di non aver attivato il blocco delle maiuscole durante la digitazione della password. Ricordate, inoltre, che il computer distingue fra caratteri maiuscoli e minuscoli, per cui* rantolo *e* Rantolo *non sono equivalenti.*

Ripetete la stessa procedura per la password dell'utente (*User*), dando preferibilmente una password diversa. Al termine, scegliete l'opzione che salva le modifiche (*Save and exit Setup*, o una dicitura equivalente) e soprattutto **ricordatevi le password**. Se le dimenticate, neppure voi potrete accedere al computer.

> ***Usate delle password non ovvie**: niente date di nascita, nomi di partner, gatti, o personaggi preferiti. Le password vanno **memorizzate** e non vanno scritte su un foglietto accanto al monitor o sotto la tastiera: lo fanno tutti e gli intrusi non sono scemi. Il consiglio vale per tutte le password che usate, qui e altrove.*

Fatto questo, ogni volta che accendete il computer, vi verrà chiesta una password e potrete usare il PC soltanto se la immettete correttamente, rispettando maiuscole e minuscole. Se avete definito due password, il computer si avvierà con una qualsiasi delle due. La differenza fra le due è che normalmente soltanto la password del supervisore permette di accedere alla modifica delle password del computer.

Alt ai dischetti traditori

Già che state accedendo al BIOS, vi conviene modificarne un'altra opzione: la *sequenza di avvio* (*boot sequence*). Normalmente, il computer tenta di partire cercando prima un sistema operativo nel lettore di floppy, poi nel lettore di CD, e infine nel disco rigido. Questo significa che se lasciate nel computer un dischetto o un CD contenente un sistema operativo, quando accendete il PC verrà avviato quel sistema operativo al posto di Windows.

Come accennato, questo consente ogni sorta di intrusione e vi espone al rischio di virus autoinstallanti, talvolta presenti nei CD e nei dischetti.[115] Il BIOS è modificabile in modo da usare una se-

quenza di avvio diversa e risolvere il problema: basta dirgli di mettere al primo posto nella sequenza il disco rigido contenente Windows. L'esatta procedura dipende dal modello di computer che avete, ma è descritta nel manuale del PC.

Password sul salvaschermo

C'è un modo molto semplice per impedire che qualcuno acceda al computer dopo che l'avete acceso: una password sul salvaschermo, che si attiva se non usate il computer per qualche minuto (per esempio perché vi siete allontanati).

Questa protezione è aggirabile con opportuni programmi facilmente reperibili in Rete, ma è comunque sufficiente a scoraggiare la maggior parte dei normali curiosi.

Per attivare la password sul salvaschermo, assicuratevi innanzitutto di avere definito una password in Windows:

- *Start* > *Impostazioni* > *Pannello di controllo* > *Account utente*. Scegliete il vostro utente (di solito ce n'è uno solo) e cliccate su *Crea password.* Seguite le istruzioni sullo schermo per definire la password. Se Windows chiede di rendere privati file e cartelle, accettate.
- Se al posto di *Crea password* trovate *Cambia password*, vuol dire che avete già definito una password. Se non ve la ricordate e neppure il suggerimento offerto da Windows vi scuote la memoria, siete nei guai e ci vuole l'intervento di un esperto.

Ora che avete (si spera) una password di Windows, potete procedere all'impostazione del salvaschermo:

- *Start* > *Impostazioni* > *Pannello di controllo* > *Schermo* > *Screen Saver.*
- Scegliete il salvaschermo che preferite, scegliete il tempo di inattività dopo il quale volete che si avvii, e poi attivate la casella *Al ripristino, proteggi con password* (Figura 14.3); infine cliccate su OK. Non vi viene chiesta la password: è quella che avete definito in Windows.

In questo modo, se il mouse non viene mosso e non viene premuto nessun tasto della tastiera per un intervallo più lungo del tempo di inattività che avete specificato, parte il salvaschermo, che è disattivabile soltanto digitando la password adatta.

Attenti alla falsa sicurezza: se non impostate una password, è sufficiente premere Invio per disattivare il salvaschermo. Inoltre la password non viene chiesta affatto se lanciate il salvaschermo manualmente.[116] *Se trovate utile questa forma di protezione, vi conviene procurarvi uno degli appositi programmi reperibili nelle biblioteche della Rete, che normalmente non hanno queste limitazioni.*

Figura 14.3

Privacy tradita da una scia di bit

Moltissimi programmi tengono traccia dei file che avete aperto. Questo consente a chi usa il computer dopo di voi di farsi un'idea ben precisa di cosa avete visto, ascoltato e scritto.

Ricordo un episodio personale in cui un giovane conoscente mi chiese l'uso di un mio PC "per chattare con la morosa". Acconsen-

tii e lo lasciai solo per non reggere l'ovvio moccolo, ma fu molto educativo notare nella sezione Cronologia del browser che aveva una predilezione per i siti *hentai*. Se non sapete cosa sono, Google è a vostra disposizione. Gli impressionabili si astengano.

Il problema contrario nasce quando siete *voi* ad aver bisogno di un PC altrui, per esempio in vacanza o quando siete lontani dal vostro computer abituale. Come garantire che non rimangano tracce eloquenti dei vostri fatti personali? Come controllare che chi usa il vostro computer non abbia frequentazioni pericolose? Ecco una breve rassegna dei principali metodi per accedere a queste informazioni (e, se necessario, eliminarle).

> *Come al solito, esistono molti altri modi per carpire informazioni sui siti visitati e i file consultati. Quelli descritti qui sono soltanto i più semplici e universali. Usarli vi mette al riparo dal curiosone medio, ma non da quello esperto.*

Menu Start

Nel menu Start classico, la voce *Dati recenti* elenca tutti i file che sono stati aperti di recente. Per azzerare temporaneamente quest'elenco, cliccate con il pulsante destro su Start e scegliete *Proprietà* e la scheda *Menu di avvio*; poi cliccate sul pulsante *Personalizza* e infine sul pulsante *Cancella*. Poi cliccate su OK e ancora su OK.

Se usate la versione “plasticosa” del menu Start, invece, cliccate con il pulsante destro su Start, scegliete *Proprietà* e la scheda *Menu di avvio*, cliccate sul pulsante *Personalizza*, scegliete la scheda *Avanzate* e cliccate sul pulsante *Cancella elenco*. Se volete impedire permanentemente a Windows di ricordarsi i file aperti di recente, disattivate la casella *Elenca i documenti aperti più di recente*. Poi cliccate su OK e ancora su OK.

Browser

I browser tengono molte tracce dei siti che visitate: la procedura esatta per esaminarle o sbarazzarsene varia a seconda del browser che usate, ma ci sono alcuni principi di base validi per quasi tutti i programmi di questo genere.

- **Cronologia**. I browser tengono un "diario" dei siti visitati. Per esempio, in Internet Explorer questo diario si chiama *Cronologia* ed è accessibile scegliendo in Internet Explorer il menu *Visualizza* e le voci *Barra di Explorer > Cronologia.*
  Per purgare queste informazioni, in Internet Explorer scegliete *Strumenti > Opzioni Internet* e la scheda *Generale* e cliccate su *Cancella Cronologia.* Per evitare che la Cronologia riprenda a memorizzarle, portate a zero il numero di giorni indicato nella stessa scheda.
  In Firefox, la Cronologia è sotto *Strumenti > Opzioni > Privacy*; in Opera, è sotto *Strumenti > Preferenze > Cronologia e cache*.

- **Cache**. I browser registrano sul disco rigido una copia temporanea delle pagine visitate che si chiama appunto *cache* (si pronuncia alla francese). Questa copia rimane anche dopo che avete terminato la navigazione ed è facilmente sfogliabile usando Esplora Risorse, rivelando in estremo dettaglio il contenuto dei siti visitati.
  Per eliminare permanentemente la cache, svuotatela e impostatene a zero le dimensioni. In Internet Explorer, scegliete *Strumenti > Opzioni Internet > Generale*, e nella sezione *File temporanei Internet* cliccate su *Elimina file* e attivate l'opzione *Elimina tutto il contenuto non in linea*; poi cliccate su *Impostazioni* e portate a 1 MB lo spazio su disco da utilizzare (non si può portare a zero, quindi con Internet Explorer non si può eliminare realmente ogni traccia). In Firefox, scegliete *Strumenti > Opzioni > Privacy > Cache*, cliccate su *Svuota* e immettete zero nella casella sottostante. In Opera, scegliete *Strumenti > Preferenze > Cronologia e cache*, poi cliccate su *Svuota adesso* e scegliete *Off*.

  Questa modifica può rendere apparentemente più lenta la navigazione, perché i browser usano questi file temporanei per simulare una consultazione più rapida delle pagine Web, visualizzando le versioni memorizzate nei file temporanei anziché andare a prendere quelle presenti nei siti.

- **Completamento automatico.** Quando digitate un indirizzo in un browser, il programma spesso tenta di "indovinare" che indirizzo volete digitare e prova a completarlo automaticamente: per esempio, se digitate *"www.mi"* potrebbe proporvi diretta-

mente *www.microsoft.it.*
Le proposte di completamento del browser si basano sui siti che avete visitato: di conseguenza, se avete visitato *www.biancanevesottoinani.com* (è solo un esempio ipotetico), quando digitate *www.bi* viene riproposto quest'indirizzo dall'aria molto discutibile. Questo consente, digitando *www* seguito da una sola lettera, di sapere tutti i siti visitati il cui nome inizia con quella lettera (Figura 14.4).
In Internet Explorer, questo rischio privacy si elimina quando si elimina la Cronologia, come descritto prima. In Firefox, si preme Maiusc-Canc per eliminare un singolo sito indesiderato dal menu a tendina del completamento automatico, oppure si sceglie *Strumenti* > *Opzioni* > *Privacy* e si clicca su *Elimina tutto* (ma in questo modo vengono purgate tutte le informazioni personali, comprese le password dei siti). In Opera, si sceglie *Strumenti* > *Preferenze* > *Cronologia e cache* e si mette a zero il valore di *Indirizzi digitati* e di *Indirizzi visitati*, cliccando anche *Cancella* in entrambe le voci.

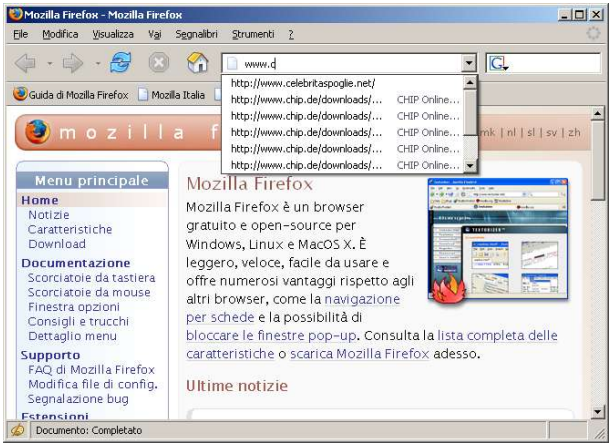

Figura 14.4

Windows Media Player

Normalmente, Windows Media Player tiene traccia dei nomi degli ultimi CD, DVD e file audio o video che sono stati visti o ascoltati: per elencarli è sufficiente cliccare sul menu File. Se volete far sparire quest'indicazione:

- in Windows Media Player, scegliete il menu Strumenti e la voce Opzioni;
- nella scheda *Privacy*, cliccate su *Cancella cronologia, Cancella CD/DVD* (o *Cancella cache*, a seconda della versione)[117] e disattivate la casella *Salva la cronologia file e URL nel lettore*.

> *Le versioni precedenti di Windows Media Player non sono altrettanto facili da personalizzare. È necessario modificare il Registro, come descritto nel capitolo supplementare* Per veri smanettoni *reperibile su* www.attivissimo.net.

Se usate un altro programma al posto di Windows Media Player, ricordatevi che potrebbe avere una "memoria" analoga dei file aperti.

I pericoli dei documenti Word

C'è una regola del Dodecalogo che probabilmente vi ha lasciato più perplessi del consueto:

> ***Regola 11: Non distribuite documenti Word: trasportano virus e contengono vostri dati personali nascosti.***

Questa, infatti, può sembrarvi la regola più difficile da seguire. Come è possibile fare a meno di distribuire documenti Word? *Tutti* usano Word!

In realtà esistono delle alternative validissime. Permettetemi una breve parentesi per mostrarvi quanto sia importante adottarle ovunque possibile e usare alcuni accorgimenti se dovete proprio diffondere un documento usando il formato Word.

Tony Blair e la privacy a rischio

In molte versioni, Microsoft Word **non purga dal file salvato le parti di testo cancellate durante la redazione del documento**, soprattutto se si usa un'opzione chiamata *salvataggio veloce*. Se un documento scritto con Microsoft Word viene distribuito in forma elettronica (ad esempio su un floppy, o pubblicandolo su Internet o inviandolo come allegato a un e-mail), chi lo scarica o riceve può leggere anche le versioni cancellate del documento, con tutte le sue modifiche intermedie, che possono essere molto rivelatrici.

Per esempio, immaginate di scrivere al vostro capo, in un momento di esasperazione, un documento Word contenente le parole *"Signor direttore, lei è un cretino"*. Prima di spedirglielo via e-mail, ci ripensate e correggete: *"Signor direttore, lei è un esempio per tutti noi"*. Carriera salva? Dipende: se il vostro capo effettivamente non è un cretino ma sa qualcosa d'informatica, apre il documento con il Blocco Note di Windows e ci trova dentro ancora l'insulto (Figura 14.5).

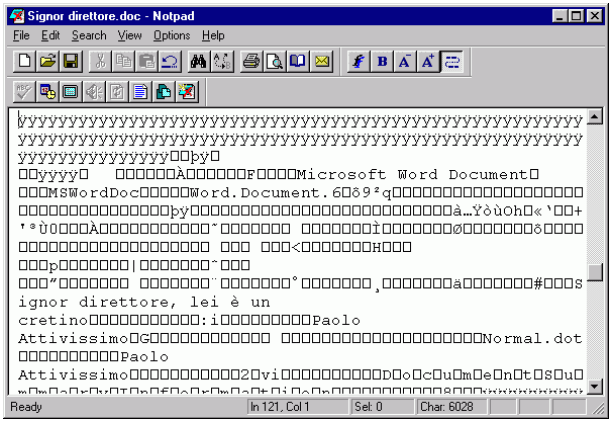

Figura 14.5

I documenti Word contengono anche molte altre informazioni che potreste trovare imbarazzanti. Per ammissione della stessa Microsoft, contengono *"il vostro nome, le vostre iniziali, il nome della vostra società o organizzazione, il nome del vostro computer, il nome del server di rete o del disco rigido sul quale avete salvato il documento, altre proprietà del file e informazioni riepilogative, porzioni non visibili di oggetti OLE embedded, i nomi degli autori pre-*

cedenti, le revisioni e le versioni del documento, informazioni sul modello, testo nascosto e commenti".[118]

Questo tipo di gaffe succede più spesso di quanto potreste pensare, e a volte tocca livelli molto delicati. Per esempio, nel settembre 2003 il primo ministro britannico Tony Blair si è trovato in grave imbarazzo quando un documento Word sulle (presunte) armi di distruzione di massa irachene ha rivelato i nomi e cognomi delle persone altolocate del governo Blair che avevano letto e approvato il testo. Questo gli ha reso impossibile prendere le distanze dal documento quando si è rivelato un'accozzaglia di scopiazzature da articoli reperibili su Internet anziché un rapporto dei servizi segreti.

Per farvi un'idea di quanto siano dettagliate le informazioni annidate nei documenti Word, nel caso Blair fu trovata traccia del nome di chi ne diede copia a Colin Powell e fu possibile accertare che lo fece usando un dischetto.[119] [120]

Se volete verificare quanto sia diffusa l'abitudine di far circolare documenti Word contenenti correzioni molto rivelatrici e altri dati "segreti", potete usare il programma gratuito *Docscrubber* (presso *www.docscrubber.com*) per analizzare il contenuto dei file Word che ricevete. Ne vedrete delle belle.

Dopo l'episodio increscioso di Blair, Microsoft ha pubblicato un programma gratuito che "ripulisce" i file Word (e anche quelli di Excel e PowerPoint). Si chiama *Rhdtool.exe* e lo trovate sul sito Microsoft cercando *"Strumento per la rimozione dei dati nascosti"*.[121] Anche il già citato Docscrubber consente una certa ripulitura dei documenti Word. Tuttavia questo rimane un approccio molto macchinoso. È molto meglio usare direttamente programmi che non salvano questi dati nascosti.

Virus e altre bestiacce nei file Word

Può sembrare assurdo infettare il computer *aprendo un documento*, ma il fatto è che con Word si può. I documenti Word, infatti, sono sempre più simili a veri e propri programmi attivi che a rappresentazioni passive di un testo. Purtroppo questa è una tendenza non circoscritta al programma Microsoft: ne risentono anche altri programmi analoghi.

Per esempio, è possibile inserire in un documento Word delle istruzioni, chiamate in gergo *macro*, che eseguono automaticamente varie operazioni. Questo è molto comodo per creare documenti interattivi, ma consente anche a un documento di cancellare file e combinare altri guai del genere quando viene aperto con Word. Ricevere un documento Word allegato a un e-mail, insomma, è come ricevere un virus: ci vuole molta cautela nell'aprirlo.

Per risolvere almeno in parte questo problema, Microsoft ha aggiunto alle versioni recenti di Word un'opzione che disabilita l'esecuzione delle macro. Ma i creatori di virus (o più correttamente *macrovirus*) si sono fatti furbi e hanno trovato il modo di disabilitare la disabilitazione, per cui i documenti Word continuano a essere pericolosi.[122] [123] [124]

> *Per verificare lo stato della gestione delle macro in Word, scegliete in Word il comando* Strumenti > Macro > Protezione*. La protezione deve essere regolata su* Elevata*.*

Inoltre Word non controlla la struttura dei documenti che gli fate aprire. Di conseguenza, è abbastanza semplice confezionare un documento strutturato in modo scorretto, che dato in pasto a Word lo manda in tilt e consente di eseguire istruzioni a piacimento sul computer della vittima.[125]

> *Un'altra ragione per cui è opportuno non essere disinvolti nell'uso del formato Word è che* ***non tutti gli utenti di computer sono in grado di leggerlo****. Ora che iniziano a diffondersi alternative a Windows e Microsoft Office e che sono stati introdotti dei pur blandi sistemi anticopia in questi programmi, infatti, non si può più dare per scontato che il destinatario di un documento possieda Word.*

Contenere l'ansia

Per evitare tutte queste preoccupazioni di sicurezza, si può ridurre al minimo indispensabile l'uso dei documenti Word. Questo è più facile di quel che potrebbe sembrare: infatti moltissimi utenti usano Word per diffondere documenti che non hanno alcuna ragione di essere composti con questo programma.

L'esempio classico è costituito dall'e-mail: capita spessissimo di ricevere allegati Word che contengono soltanto del testo semplice, che sarebbe stato perfettamente leggibile anche se immesso nel corpo del messaggio. C'è addirittura chi invia un'immagine inserendola in un file di Word, quando sarebbe stato infinitamente più semplice inviarla tal quale.

È una vera e propria Wordmania dilagante, che obbliga il destinatario ad aprire inutilmente il programma Microsoft (ammesso che lo possieda) oppure, visti i problemi dei file Word, a cancellare l'allegato per paura di virus e altre delizie o semplicemente perché non può leggerlo (Microsoft fornisce un programma di lettura gratuito, ma soltanto per Windows).

Il primo passo per curare questa mania è **non usare il formato Word quando non è necessario.** Se dovete spedire un'immagine, speditela e basta: non c'è motivo di incartarla dentro un documento Word. Se dovete inviare un testo privo di impaginazione ed effetti grafici, mandatelo direttamente nel corpo del messaggio. Noterete, fra l'altro, che in questo modo i messaggi saranno molto più leggeri e peseranno meno sulla bolletta (vostra e del destinatario).

Il secondo passo è **usare il formato PDF** per tutti i documenti che non devono essere modificati dal destinatario. Questo approccio ha numerosi vantaggi:

- **maggiore garanzia d'integrità**. Avete mai considerato che chiunque potrebbe prendere un vostro documento Word, magari con tanto di firma e logo aziendale, modificarlo e poi spacciarlo per autentico? Alterare un documento in formato PDF è possibile, ma non è alla portata di tutti come lo è una modifica di un file Word.
- **maggiore universalità.** Esistono programmi di lettura gratuiti per il formato PDF utilizzabili su qualsiasi tipo di computer: Linux, Mac, tutte le versioni di Windows, Solaris, OS/2, computer palmari e persino alcuni telefonini. Il principale programma gratuito per Windows è *Adobe Reader* (*www.adobe.com*).
- **maggiore compatibilità.** La corretta visualizzazione di un documento Word sul computer del destinatario richiede non solo che il destinatario abbia Word, ma anche che disponga di tutti i *font* (tipi di carattere) che avete usato nel documento. Se un carattere non è disponibile, la vostra impaginazione tanto cura-

ta va a farsi benedire, a meno che vi ricordiate di attivate l'apposita opzione di Word che include i font nei documenti, cosa che fanno in pochi.[126] Con il formato PDF, invece, i font sono inclusi automaticamente nel documento, per cui il problema non si pone: il destinatario vede il documento esattamente come l'avete realizzato.

- **nessun dato personale o segreto nascosto di cui preoccuparsi.** Il formato PDF non include dati sulle modifiche precedenti del documento o altri identificativi personali.
- **minore rischio virus.** È teoricamente possibile infilare un comando ostile in un documento PDF, ma soltanto in circostanze particolari.[127] È comunque consigliabile, come sempre, un esame con un antivirus aggiornato.

Generare un documento in formato PDF è facile: potete farlo persino usando Word. Basta aggiungere al computer un apposito programma, che si integra nel menu di stampa di Word e di tutti gli altri programmi del vostro PC: ce ne sono per tutte le tasche (anche quelle vuote). Ecco qualche esempio:

- **Acrobat** di Adobe
  www.adobe.it/products/acrobat/main.html
  A pagamento
- **Pdf995**
  www.pdf995.com
  Gratuito con pubblicità, 9 dollari e 95 senza pubblicità
- **PDF Creator**
  sourceforge.net/projects/pdfcreator/
  Gratuito e libero
- **CutePDF Writer**
  www.acrosoftware.com/Products/CutePDF/writer.asp
  Gratuito

Trovate altri programmi gratuiti o a pagamento per generare e leggere file PDF presso siti come *www.pdfzone.com*. In alternativa, potete usare uno dei tanti servizi di conversione online (reperibili digitando *"convert to pdf"* in Google), compreso quello di Adobe, oppure adoperare il programma gratuito *OpenOffice.org,* che include direttamente l'opzione di salvare i documenti in formato PDF (è il programma che ho usato per scrivere questo libro e pubblicarlo su Internet appunto in formato PDF).

Se vi state chiedendo come mai non consiglio il formato RTF, piuttosto diffuso come alternativa a Word, la ragione è semplice: è un formato troppo poco standard. Documenti generati da programmi diversi (o da versioni diverse dello stesso programma) sono spesso incompatibili o producono impaginazioni differenti, e non risolvono il problema dei font. L'RTF, insomma, offre poche garanzie di universalità e di completezza.

Capitolo 15

Rimedio radicale: l'alternativa Mac e Linux

Sorpresa! In realtà, oltre alle dodici regole del Dodecalogo, ce ne sarebbe una tredicesima:

> ***Se potete, non usate Windows****: usate sistemi operativi alternativi come Linux, Mac OS, BSD, QNX e altri ancora.*

Lo so, questa regola non c'è nell'elenco sintetico. La aggiungo qui, a fine libro, perché è un po' estrema e radicale rispetto alle altre. Ma è la più efficace, anche se impegnativa da mettere in pratica.

Le ragioni di questa regola sono fondamentalmente due:

- **Praticamente tutti gli attacchi informatici sono mirati a sfruttare le vulnerabilità del software Microsoft**, perché è il più diffuso e quindi offre il maggior numero di vittime potenziali, e perché è intrinsecamente più difficile creare un virus per gli altri sistemi operativi. Usando i sistemi operativi alternativi evitate sostanzialmente il problema virus (con eccezioni talmente rare da essere trascurabili)**.**
- **Il software Microsoft è notoriamente più ricco di vulnerabilità critiche rispetto alle alternative.** Lo testimonia il numero di *patch* di correzione che Microsoft è costretta a sfornare per i componenti vitali di Windows (incluso Internet Explorer, che è parte integrante del sistema operativo).

Lo so che è una proposta radicale e apparentemente insensata, ma il fatto è che usare un sistema operativo diverso da Windows elimina in un sol colpo praticamente tutti i problemi di sicurezza e di continuo aggiornamento che avete con Windows.

Riflettete su questo:

- **Linux** ormai offre sostanzialmente tutte le stesse potenzialità e applicazioni di Windows, a patto di studiare un po', e a prezzo bassissimo (praticamente zero, visto che è scaricabile gratis e funziona sul PC che avete già).

- Il **Mac** le offre con meno studio, ma a un prezzo un po' più alto e a condizione di cambiare computer.
- Linux è conveniente se il vostro tempo è a buon mercato; se di tempo ne avete poco, vi conviene il Mac, dove tutto funziona al primo colpo e potete persino continuare a usare Microsoft Office: infatti ce n'è un'ottima versione per questo sistema operativo.
- Nessun virus o allegato infetto può farvi nulla se il vostro computer Linux o Mac è correttamente configurato. La cosa interessante è che i sistemi operativi alternativi sono preconfigurati correttamente per la sicurezza: escono blindati dalla fabbrica. Windows, invece, ha bisogno di[128] un lungo lavoro di irrobustimento.

Se vi interessa saperne di più su Linux, potreste cominciare dalla guida introduttiva che ho scritto, intitolata *Da Windows a Linux,* che potete scaricare gratuitamente dal mio sito.

Se volete conoscere meglio il Mac, chiedete a qualche amico che ce l'ha di farvi una dimostrazione, e datemi un po' di tempo: ne parlerò in un prossimo libro. Infatti, stanco di Windows, ho da poco migrato tutto il mio lavoro informatico a quest'alternativa. L'unico rimpianto è non averlo fatto prima.

E voi cosa aspettate?

Glossario

Ho cercato di tenere a bada il gergo tecnico, ma capisco che sia facile perdersi fra tutti questi paroloni di origine quasi sempre straniera. Eccovi un piccolo glossario da consultare per rinfrescarvi la memoria se trovate un termine misterioso durante la lettura.

adware. Un programma che inietta pubblicità nel computer.

area di notifica. La zona in basso a destra della barra delle applicazioni di Windows.

autoplay. Funzione di Windows che suona automaticamente i CD musicali ed esegue altrettanto automaticamente i DVD.

autorun. Funzione di Windows che avvia automaticamente i programmi contenuti su CD e DVD.

backup. Copia di sicurezza di dati e/o programmi.

boot virus. Virus che si attiva all'avvio del computer.

browser. Programma per navigare nelle pagine del Web. Esempio classico: Internet Explorer.

cartella. Una suddivisione del vostro disco rigido, che può contenere file di vario genere, come un cassetto di uno schedario.

chat. Modo di comunicare istantaneamente via Internet tramite messaggi di testo.

cleaner. Programma antivirus specificamente progettato per eliminare uno o più virus specifici da un computer già infetto.

cracker. Imbecille che devasta i computer e i siti Web per denaro o per vandalismo.

dialer. Programma che tenta di cambiare più o meno di nascosto il numero di telefono composto per collegarsi a Internet, sostituendolo con un costosissimo numero a pagamento.

directory. Lo stesso che *cartella*.

estensione. Il suffisso in coda ai nomi dei file. Nel nome di file *documento.sxw*, *sxw* è l'estensione.

exploit. Dimostrazione pratica di una falla di sicurezza.

firewall. Programma o dispositivo che filtra il traffico ostile o a rischio proveniente da Internet o uscente dal vostro computer.

groomer. Molestatore che coltiva e prepara con cura l'attacco alle proprie vittime.

hacker. Secondo i giornalisti, lo stesso che *cracker*. Secondo gli informatici, uno smanettone: una persona che ama trovare usi creativi ma innocui per la tecnologia.

HTML. Il linguaggio informatico usato per comporre le pagine di Internet e (purtroppo) l'e-mail piena di effetti grafici.

keylogger. Programma o dispositivo che registra e inoltra al suo padrone tutto quello che viene digitato dalla vittima sorvegliata.

link. Rimando o collegamento verso una pagina di Internet o verso un indirizzo di posta.

memoria USB. Dispositivo ultracompatto per portare in giro notevoli quantità di dati. Sta sostituendo sempre più spesso i dischetti.

newsgroup. Area di Internet dedicata alle discussioni a tema, accessibile tramite appositi programmi o tramite Google Gruppi (*groups.google.it*).

nickname. Pseudonimo usato da un utente di Internet per brevità, per farsi riconoscere o per diventare anonimo e *non* farsi riconoscere.

patch. Aggiornamento-correzione di un programma o sistema operativo.

phishing. Truffa via Internet, che consiste nel mandare a milioni di utenti falsi e-mail che sembrano provenire da società rispettabili ma in realtà portano chi abbocca a consegnare i propri dati segreti ai truffatori.

popup. Pagina pubblicitaria che compare a sorpresa sopra quella che stiamo leggendo.

RAM. La memoria temporanea del computer, usata come area di lavoro.

social engineering. L'arte truffaldina di manipolare le emozioni delle persone per far loro abbassare le difese.

spam. Pubblicità indesiderata diffusa via e-mail.

spammer. La feccia che dissemina lo *spam*.

spyware. Programma che comunica segretamente a terzi l'attività svolta al computer dalla sua vittima, per spionaggio o per raccogliere dati statistici.

systray. Lo stesso che *area di notifica*.

tabbed browsing. Funzione presente in tutti i programmi di navigazione evoluti, che consente di accedere più facilmente a una specifica pagina Web fra le tante che abbiamo visualizzato.

trojan horse. Virus che si spaccia per un programma utile o divertente ma ha in realtà un secondo fine.

virus. *In questo libro*, qualsiasi programma che si intrufola nel computer di una vittima per fare danni e si propaga da un computer all'altro con o senza l'aiuto dell'utente.

web bug. Piccolissima immagine inclusa sotto forma di *link* in un e-mail per consentire il tracciamento a distanza di un messaggio e sapere quando viene aperto e chi lo apre.

webmail. Metodo per usare l'e-mail tramite il *browser* invece di usare un programma apposito.

worm. Un virus con le gambe. In altre parole, un programma ostile che è in grado di propagarsi da un computer all'altro senza richiedere l'intervento della vittima.

Capitolo supplementare

Note a fine testo

Le note che trovate nelle pagine successive non fanno parte del testo definitivo su carta: erano nate soltanto come miei appunti di lavorazione, ma poi ho pensato che potrebbero esservi utili, per cui ho pensato di lasciarne traccia nella versione elettronica del libro.

Essendo semplici appunti, vi trovate un po' di tutto, comprese citazioni in inglese e sgrammaticature degli originali. Non scandalizzatevi.

1. Jargon file, "virus": A cracker program that searches out other programs and `infects' them by embedding a copy of itself in them, so that they become Trojan horses. When these programs are executed, the embedded virus is executed too, thus propagating the `infection'. This normally happens invisibly to the user. Unlike a worm, a virus cannot infect other computers without assistance. It is propagated by vectors such as humans trading programs with their friends (see SEX). The virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things like writing cute messages on the terminal or playing strange tricks with the display (some viruses include nice display hacks). Many nasty viruses, written by particularly perversely minded crackers, do irreversible damage, like nuking all the user's files. In the 1990s, viruses have become a serious problem, especially among IBM PC and Macintosh users (the lack of security on these machines enables viruses to spread easily, even infecting the operating system). The production of special anti-virus software has become an industry, and a number of exaggerated media reports have caused outbreaks of near hysteria among users; many lusers tend to blame *everything* that doesn't work as they had expected on virus attacks. Accordingly, this sense of `virus' has passed not only into techspeak but into also popular usage (where it is often incorrectly used to denote a worm or even a Trojan horse). See phage; compare back door; see also UNIX conspiracy.
2. Jargon file, "worm": [from `tapeworm' in John Brunner's novel "The Shockwave Rider", via XEROX PARC] n. A program that propagates itself over a network, reproducing itself as it goes. Compare virus. Nowadays the term has negative connotations, as it is assumed that only crackers write worms. Perhaps the best-known example was Robert T. Morris's `Internet Worm' of 1988, a `benign' one that got out of control and hogged hundreds of Suns and VAXen across the U.S. See also cracker, RTM, Trojan horse, ice, and Great Worm, the.
3. La lista ufficiale pubblicata da Microsoft è presso support.microsoft.com/default.aspx?scid=kb;en-us;884130
4. www.informationweek.com/story/showArticle.jhtml?articleID=21401332.
5. www.accademiadellacrusca.it/faq/faq_risp.php?id=3937&ctg_id=44: *E-mail* è la forma abbreviata per *Electronic mail* cioè "posta elettronica". Il sostantivo che funge da testa nel composto è *mail*, che pone il solito problema per quel che riguarda la definizione del genere: la differenza principale tra i due sistemi sostantivali risiede infatti nel genere, che è naturale nell'inglese e grammaticale nell'italiano. In inglese anche *mail* è neutro e in italiano trova dei corrispondenti in "posta" e "corrispondenza" femminili. **Anche nel recente *Grande dizionario italiano dell'uso* di Tullio De Mauro la parola *e-mail* è indicata come sostantivo femminile invariabile**. Il femminile si ha spesso per analogia semantica, cioè un prestito riceve il genere di un sostantivo nella lingua ricevente che ha un

significato affine (es. la star, la gang, la performance, la nomination). **È però abbastanza diffusa l'alternanza,** per quel che concerne il genere, nell'uso di questo termine e questa incertezza ritengo sia prodotta da due principali fattori:
1) La presenza di altri termini inglesi formati che hanno acquisito il genere maschile dal neutro inglese, considerato come genere più adattabile al maschile in quanto comunque meno marcato, in italiano, rispetto al femminile.
2) Il corrente uso metonimico cui è sottoposto il termine, per cui **dal più generale "posta elettronica" è arrivato immediatamente ad indicare il singolo "messaggio"** inviato tramite posta elettronica. In questo processo entra in gioco una nuova parola "messaggio" (peraltro molto diffusa anche nella forma "messaggino" per indicare i brevi testi che si inviano con i cellulari) che introduce il genere maschile e genera confusione e incertezza (in particolare in chi non conosce l'inglese), insinuando il dubbio, che può essere rafforzato anche dalla casualità per cui le due parole hanno anche la stessa iniziale, che ***mail* abbia come forma corrispondente italiana *messaggio*, quindi una parola di genere maschile.**

6. news.com.com/Major+graphics+flaw+threatens+Windows+PCs/2100-1002_3-5366314.html.
7. www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200; www.microsoft.com/technet/security/bulletin/ms04-028.asp
8. Secondo l'Anti-Phishing Working Group (Apwg) (www.antiphishing.org/), nel periodo tra gennaio e febbraio i casi di phishing sono aumentati del 60 per cento, arrivando a quota 2,3 miliardi in un solo mese (Repubblica.it: www.repubblica.it/2004/c/sezioni/scienza_e_tecnologia/truffawe/truffawe/truffawe.html; la cifra di 2.3G non è confermata presso l'APWG)
9. www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.
10. www.microsoft.com/technet/security/current.aspx.
11. europa.eu.int/comm/competition/antitrust/cases/decisions/37792/en.pdf.
12. Il filmato è disponibile presso www.cnn.com/TECH/computing/9804/20/gates.comdex/.
13. www.theinquirer.net/?article=6811: Vole says: "An attacker could seek to exploit this vulnerability by creating an .MP3 or .WMA file that contained a corrupt custom attribute and then host it on a website, on a network share, or send it via an HTML email. If a user were to hover his or her mouse pointer over the icon for the file (either on a web page or on the local disk), or open the shared folder where the file was stored, the vulnerable code would be invoked. An HTML email could cause the vulnerable code to be invoked when a user opened or previewed the email. A successful attack could have the effect of either causing the Windows Shell to fail, or causing an attacker's code to run on the user's computer in the security context of the user."
14. Un elenco più completo delle estensioni a rischio è disponibile presso antivirus.about.com/library/blext.htm.

15. www.sophos.com/virusinfo/analyses/w32mypartya.html
16. Link files (*.lnk) can take you to an evil website with malicious active content. The others can contain hostile content which is activated when you open the file.
17. *A clever way to use a SHS file: Make a copy of CALC.EXE and put it on your desktop. Open Wordpad. Click and drag calc.exe into the open wordpad document. Click and drag it back to the desktop. Rename the file that it created (Scrap) to Readme.txt. You now have what appears to be a text document icon and a clearly named readme.txt file showing on your desktop. Click on the text file and the notepad opens up. If this were a trojan, you would have been fooled and infected by what seemed to be a harmless text file. If the extension was allowed to be seen you would not have been fooled by the file Readme.txt.shs.* I file con l'estensione "shs" sono particolarmente pericolosi, come dimostrato dal virus "Life Stages", che camuffava un virus in quello che sembrava essere un file di testo innocuo in formato txt. SHS sta per Shell Scrap: è un residuo del vecchio Windows 3.1. Consente di includere in uno pseudo-documento Word qualsiasi file, anche un eseguibile, in modo tale che il computer lo apra automaticamente. Il file SHS ha un'icona simile a quella del Blocco Note. Vedi anche: www.pc-help.org/security/scrap.htm, www.geocities.com/floydian_99/inv3.html
18. www.geocities.com/floydian_99/inv3.html: The most known file type that is invisible is .SHS, since the "Life Stages" virus used this "feature" to camouflage a virus in what looked like an innocent .TXT ascii file. But the most common invisible file type is used by practically everybody, and that is the .LNK, which are the shortcuts you use on your desktop or menus to open up applications and files. We use to take these shortcuts as an object of the operating system, but in fact they are only small files, with a hidden .LNK extension appended to it. So, back to .SHS, it stands for Shell Scrap. It's an old dinosaur from Windows 3.1 that was mostly unknown until only a couple of years ago. It is used for OLE (Object Linking and Embedding), and using a Shell Scrap, you can just include any file you want, even an executable, in a Word document, for example, and the system will open it for you. The .SHS file will bear an icon resembling somewhat the one of Notepad, but still slightly different (the bottom of the page is ripped). The .SHS extension itself is invisible, as we said, so you can make it look like it is something else. For an excellent overview of Shell Scraps, see www.pc-help.org/security/scrap.htm.
19. More about CLSIDs here: www.geocities.com/floydian_99/inv4.html
20. cybercoyote.org/security/safe-ext.htm
21. www.techtv.com/callforhelp/answerstips/story/0,24330,419,00.html
22. In XP Pro (in XP Home non c'è gpedit.msc) si può fare così: Start > esegui, scrivere "gpedit.msc" e premere invio; andare alla voce "Configurazione utente" > "Modelli amministrativi" > "Sistema" > "Disattiva riproduzione automatica", cliccarci sopra due volte,

selezionare "Attivato" e premere "OK". Funziona sia con Win2000 che con XP, sia con i CD che con le periferiche USB (nota di un lettore).

23. PowerToys will only work with US-English regional settings. Version 2.10 requires Windows XP Service Pack 1 or Windows Server 2003
24. Per impedire soltanto l'esecuzione automatica di dischi contenenti musica, immagini e video (ma non quella di programmi) senza dover toccare il Registro: in Esplora Risorse, cliccate con il pulsante destro sull'icona del lettore e scegliete *Proprietà*. Nella scheda *Autoplay*, scegliete il tipo di CD/DVD di cui volete disabilitare l'esecuzione automatica e scegliete *Selezionare l'operazione da eseguire* e poi *Nessuna operazione*; infine cliccate su *Applica*. Ripetete questo passo per ciascun tipo di CD/DVD che vi interessa disabilitare, poi cliccate su OK; la modifica ha effetto su tutti i lettori e masterizzatori di CD e DVD del vostro computer, se ne avete più di uno.
25. www.stopmessengerspam.com/windows_xp/windows_xp.html; www.netsquirrel.com/messenger/; idg.net.nz/news.nsf/UNID/6D0CCDEC34540FAFCC256DD600731DB4?OpenDocument
26. www.microsoft.com/technet/security/bulletin/MS03-043.mspx
27. www.securityfocus.com/bid/5478/exploit
28. www.securiteam.com/windowsntfocus/6Q00K0K5SI.html
29. Disabilitandolo, il LiveUpdate Automatico di Norton AV 2004 risulta disattivato senza possibilità di riattivarlo, e la scansione pianificata dello stesso AV sembrerebbe non funzionare più (nota di Luca Martino).
30. Elenco dettagliato dei ruoli e dei settaggi consigliati per i vari servizi, pre e post SP2: www.blackviper.com/WinXP/servicecfg.htm
31. support.microsoft.com/default.aspx?scid=kb;EN-US;Q306203
32. Si chiama formalmente così la suite gratuita per ufficio: tutti la chiamano *OpenOffice*, ma *OpenOffice* è un marchio registrato di un'altra società: "Because of trademark issues, OpenOffice.org must insist that all public communications refer to the project and software as "OpenOffice.org" or "OpenOffice.org 1.0," and not "OpenOffice" or "Open Office."" (www.openoffice.org/about_us/summary.html)
33. www.boston.com/business/technology/articles/2004/06/09/home_pcs_big_source_of_spam/
34. www.samspade.org/d/firewalls.html
35. www.kb.cert.org/vuls/id/713878
36. Anche quelli hardware: Symantec corregge alcune vulnerabilita' che potevano consentire ad un cracker di bloccare il funzionamento di alcune firewall appliance o modificarne la configurazione URL: punto-informatico.it/pi.asp?i=49763
37. punto-informatico.it/pi.asp?i=49661; www.pcwelt.de/know-how/extras/103039/; www.megalab.it/news.php?id=294
38. www.microsoft.com/italy/windowsxp/using/security/internet/sp2_wfintro.mspx
39. www.xtra.co.nz/help/0,,6156-3602209,00.html#2

40. www.microsoft.com/italy/windowsxp/using/security/internet/sp2_wfsettings.mspx
41. "Windows Firewall will automatically allow all outbound connections, regardless of the program and the user context" (from MS's .DOC files)
42. Un esempio per tutti è il famigerato *Sasser.*
43. www.theregister.co.uk/2004/09/22/opt-out_exploit/
44. Un lettore riferisce, per esempio, che ha avuto una pessima esperienza con l'antivirus di Norton versione 2002: l'AV 2002 non va su XP, e non ha rilevato un virus presente su un PC. Lo stesso virus è stato rilevato da un servizio di scan online.
45. Sono DLL. Come si disinstallano? Non si sa, sui siti degli antivirus online non c'è scritto. Metodo brutale: identificare le DLL, scoprire in quale directory sono state piazzate, aprire un prompt e digitare **regsvr32 /u nomedelfile.dll** (che dovrebbe disinstallare la DLL dal Registro) poi cancellare la DLL dal disco.
46. Alcuni antivirus, come il Norton 2004, richiedono che sia attivo il servizio *Utilità di pianificazione*.
47. Un modo per aggiornare manualmente Norton Antivirus 2004 è prelevare il relativo file seguendo il link del sito web del produttore: www.symantec.com/avcenter/download/pages/IT-N95.html (segnalazione di Luca Martino)
48. www.microsoft.com/italy/technet/solutions/security/falsi_bolletini.asp (sì, *bolletini* con una T sola)
49. La pagina spiega fra l'altro come capire quando un e-mail che apparentemente ha come mittente Microsoft è in realtà fasullo: *"Il messaggio non è firmato tramite la chiave PGP del Microsoft Security Response Center. Prima di inviare i bollettini,* ***Microsoft appone sempre una firma digitale*** *che è possibile controllare utilizzando la chiave pubblicata all'indirizzo www.microsoft.com/technet/security/bulletin/notify.asp. In caso di dubbi sull'autenticità di un bollettino ricevuto per posta elettronica, è possibile confrontarlo con le versioni ufficiali dei bollettini pubblicate sul sito Web Microsoft TechNet."* [...] *"I* ***bollettini autentici non contengono mai un collegamento a una patch****, ma rimandano alla versione completa del bollettino pubblicata sul sito Web di Microsoft, in cui è disponibile il collegamento alla patch."*
50. Ecco qualche esempio di queste notifiche misteriose, tratte dalla mia collezione personale:

```
Da: "System Anti-Virus Administrator" <postmaster@[omissis]
>
A: <[vostro indirizzo di e-mail]>
Oggetto: virus found in sent message "Re: Your website"
Data: lunedì 22 marzo 2004 8.12
Attention: [vostro indirizzo di e-mail]
A virus was found in an Email message you sent.
This Email scanner intercepted it and stopped the entire
message reaching its destination. The virus was reported to
be: Worm.SomeFool.Gen-1
Please update your virus scanner or contact your IT support
personnel as soon as possible as you have a virus on your
```

```
system.
Your message was sent with the following envelope:
MAIL FROM: [vostro indirizzo di e-mail]
RCPT TO: [indirizzo di un utente a voi sconosciuto]
[...]
-----------
V I R U S A L E R T

Our viruschecker found a VIRUS in your email to
"[omissis]".
We stopped delivery of this email!

Now it is on you to check your system for viruses

For further information about this viruschecker see:
http://amavis.org/
AMaViS - A Mail Virus Scanner, licenced GPL
---------------
From: Postmaster <postmaster@[omissis]>
To: <topone@pobox.com>
Date: Mon, 22 Mar 2004 10:09:49 +0100 (CET)
X-Virus-Scanned: by amavisd-new

------------------------------
NETCOMPANY Antivirus results
------------------------------

Il file infetto e' stato salvato in quarantena con il nome:
virus-20040322-100949-XXMcn9FU .
The infected file was saved to quarantine with name:
virus-20040322-100949-XXMcn9FU .

Il file allegato alla e-mail (con Oggetto: information )
inviata da
<topone@pobox.com> a [omissis], e' infettata dal virus:
WORM_NETSKY.B .

The file attached to mail (with subject: information ) sent
by
<topone@pobox.com> to [omissis] is infected with virus:
WORM_NETSKY.B .
```

51. www.apogeonline.com/webzine/2004/02/04/01/200402040101#Inizio Pagina
52. www.pcstats.com/articleview.cfm?articleid=1643&page=2: In Windows XP Home, **the built-in 'administrator' account is only available in safe mode** and is the default account for that mode. **The password for the administrator account is blank**, since it is not accessible except in safe mode. It's recommended that you log in as this account to make changes in safe mode. The fact that the administrator password is blank by default also allows you to **use XP Home's safe mode to reset the password of other user accounts** on your machine in the event that you lose the original password. Of course, this also means that every user account on your system is vulnerable to someone with direct access to the system, which is why XP Home is intended for non-business use only.

53. Lista di programmi infetti con spyware: www.fcenter.ru/Software/Miscellaneous/Spyware/spywarelist.txt
54. Kit di traduzione: www.ilsoftware.it/servizi/dl/adaware_se_ita.zip
55. www.earthlink.net/spyaudit/press/
56. news.com.com/Gates+Microsoft+to+offer+anti-spyware/2100-7355_3-5393208.html: It's also a problem that has affected Gates personally. He said his home PCs have had malware, although he has personally never been affected by a virus. "I have had malware, (adware), that crap" on some home machines, he said.
57. punto-informatico.it/p.asp?i=45808
58. Se si usa ADSL con un adattatore USB, oppure con un router configurato come Bridge Ethernet, quasi sicuramente si usa ad una connessione di tipo Dial-Up, sostanzialmente identica a quella usata con un modem tradizionale. Se usate un router vero e proprio, invece, questa vulnerabilità non c'è.
59. Il prefisso a pagamento 892 è escluso da questa disabilitazione, ma non risulta usato dai dialer, anche se lo usano i servizi di cartomanzia e affini. Anche l'164 è escluso (tariffa flat da 1 euro). È improbabile che i dialer usino questi prefissi perché hanno a disposizione soltanto 1000 combinazioni e devono passare al vaglio del Ministero delle Comunicazioni.
60. Come nota il sito dell'Autorità per le Garanzie nelle Comunicazioni, l'AGC, "con la sua delibera 78/02/CONS, ha definito le norme di attuazione dell'art. 28 del d.P.R. 77/01, stabilendo l'obbligo per gli operatori di accesso diretto di offrire il blocco selettivo di chiamata verso i tipi di chiamata e le numerazioni riportate in allegato alla delibera."
61. www.zeusnews.it/index.php3?ar=stampa&cod=3412
62. HOW TO: Back Up, Edit, and Restore the Registry in Windows XP and Windows Server 2003: support.microsoft.com/default.aspx?scid=kb;en-us;Q322756
63. news.bbc.co.uk/1/low/business/642671.stm
64. www.pcworld.com/news/article/0,aid,105144,00.asp
65. www.theinquirer.net/?article=11436
66. www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/it/default.mspx
67. "Boxed retail versions of Windows XP and SP2 will be available by the end of October [2004]". ZDNetWeek #43, p.18.
68. www.zanezane.net/articoli.asp?code=454
69. L'idea di Berners-Lee è del 1989, ma il 1991 è l'anno in cui viene presentata formalmente. Fonte: mia cronologia, atti del processo antitrust Microsoft.
70. Per esempio, la correzione "MS04-004 Cumulative Security Update for Internet Explorer (832894)", presso support.microsoft.com/default.aspx?scid=kb;en-us;Q834489, è consigliata a tutti gli utenti di Windows, compresi quelli che non usano Internet Explorer: infatti il servizio Windows Update di Microsoft dice esplicitamente, durante l'installazione della correzione, che la falla "riguarda tutti i computer che hanno Internet

Explorer installato, anche se non viene utilizzato come browser Web".

71. Altri link utili per blindare IE e OE:
    www.codecutters.org/outlook/
    www.techbargains.com/hottips/hottip13/index.cfm
    www.wintricks.it/manuali/IE6_sicurezza_web.html
    sicurezza.html.it/articoli.asp?idcatarticoli=14&Idarticoli=16&npagina=2
    www.tames.net/security/iesettings.htm
    insideoe.tomsterdam.com/
72. support.microsoft.com/?kbid=315933
73. www.securityfocus.com/bid/9628
74. Javascript vuln demo:
    www.lockdowncorp.com/bots/testyourbrowser.html
75. Java era una maniera molto promettente per creare programmi "universali", ossia indipendenti dal sistema operativo, che potessero funzionare in Windows, Linux, MacOS e persino sui telefonini, purché dotati di una cosiddetta *macchina virtuale Java* (JVM, da *Java Virtual Machine*). Microsoft, temendo che Java rendesse irrilevante Windows, incluse in Windows una versione della JVM leggermente diversa dagli standard. Improvvisamente milioni di utenti Windows si accorsero che i programmi Java non funzionavano più correttamente e diedero la colpa a Java, affossando così questa tecnologia. Risultato: niente più programmi universali, Windows salvo, e causa ultramiliardaria di Sun (società creatrice di Java) contro Microsoft, conclusasi con la condanna della società di Bill Gates e con l'eliminazione della JVM Microsoft da Windows. (java.sun.com/lawsuit/) Ora la JVM non viene più preinstallata in Windows, ma va scaricata come componente separato, e ce ne sono due versioni: quella Sun (l'originale) e quella Microsoft (piena di falle). Siccome non è preinstallata e oltretutto non si sa quale versione usare perché alcuni siti usano quella Microsoft e altri quella Sun, quasi nessuno si prende la briga di installarla (anche se alcuni browser alternativi lo fanno automaticamente). Di conseguenza, praticamente nessuno crea più attacchi basati su Java; vale comunque la pena di disattivarlo più che altro perché i programmi Java rallentano molto il computer (se dotato di macchina virtuale Java) e spesso collassano per via delle incompatibilità fra le due versioni della macchina virtuale. Microsoft, insomma, ha perso la causa, ma ha vinto la guerra, sabotando una tecnologia che poteva toglierle il monopolio. Addio Java, è stato bello conoscerti.
76. Alcuni lettori segnalano che la disattivazione del VBS dà problemi con Windows Update. "ti riporto un distinto ricordo di un po' di tempo fa: stavo installando una macchina e durante l'installazione di explorer ho deselezionato il checkmark relativo allo scripting host, ma poi ho dovuto ri-abilitarlo perché non mi andava su WU. In realtà l'inconveniente si è verificato durante la prima connessione, che notoriamente richiede il download e l'installazione della versione più aggiornata dell'uploader, ma non escludo che possa creare problemi

pure dopo, perché se WU non è un'esecuzione di script sull'host." Altri dicono che non ci sono problemi: "ho installato e configurato moltissime macchine, sia sotto Win98 / Win98SE che sotto Win2000/XP, ed il meccanismo WindowsUpdate ha sempre funzionato regolarmente anche se sulle macchine NON veniva installato il supporto Scripting Host. Non e' necessario nemmeno il VBS."

77. Spiego queste tecniche in dettaglio, con dimostrazioni pratiche, presso *www.attivissimo.net/security/bc/test10.htm* e *www.attivissimo.net/security/fakesites/fakesites.htm*.
78. secunia.com/advisories/11978 (Frame Injection Vulnerability)
79. REFUSO: nella versione cartacea manca questo *di*.
80. Dopo il Service Pack 2, IE esige che non vi siano contraddizioni fra l'estensione del nome del file, il content-type (o MIME type) e il content-disposition, e lo "sniffing" MIME (l'esame dei bit identificativi contenuti in alcuni tipi di file).
81. Info e consigli di configurazione:
    www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2brows.mspx#XSLTsection129121tt120120
    www.microsoft.com/windowsxp/using/web/sp2_addonmanager.mspx
    www.microsoft.com/windows/ie/using/howto/security/settings.mspx
    www.microsoft.com/windowsxp/sp2/ieoeoverview.mspx
    www.tames.net/security/iesettings.htm
82. Perlomeno nella versione pre-SP2, OE esegue automaticamente la musica inclusa in un messaggio.
83. Microsoft sosteneva che questa era una *feature*: news.com.com/2100-1001-964166.html?tag=rn (a proposito di Outlook, non OE, ma il concetto non cambia).
84. www.microsoft.com/technet/security/bulletin/MS01-020.mspx (marzo 2001): Because HTML e-mails are simply web pages, IE can render them and open binary attachments in a way that is appropriate to their MIME types. However, a flaw exists in the type of processing that is specified for certain unusual MIME types. If an attacker created an HTML e-mail containing an executable attachment, then modified the MIME header information to specify that the attachment was one of the unusual MIME types that IE handles incorrectly, **IE would launch the attachment automatically when it rendered the e-mail.** An attacker could use this vulnerability in either of two scenarios. She could host an affected HTML e-mail on a web site and try to persuade another user to visit it, at which point script on a web page could open the mail and initiate the executable. Alternatively, she could send the HTML mail directly to the user. In either case, the executable attachment, if it ran, would be limited only by user's permissions on the system.
85. Per esempio, i web bug funzionano anche con Eudora, se dal menu Tools > Options > Display non si toglie la spunta dalla voce "Automatically download HTML graphics".
86. 6.00.2800.1123 con tutte le patch fino al 2/10/2004. Dopo l'installazione del SP2, diventa la 6.00.2900.2180

(xpsp2_rtm.040803-2158)

87. Consente di sapere se un modulo contenuto in un e-mail HTML è sicuro o no. Se i dati che immettete nel modulo sono di natura riservata, devono viaggiare in https. Se qualcuno vi chiede di immettere dati riservati in un modulo insicuro, è un incosciente oppure un truffatore.
88. Consente di trascinare un file presente in una pagina Web o in un e-mail HTML e copiarlo al proprio computer. Ottimo per indurre una vittima a trascinare un file apparentemente innocuo che è in realtà un virus.
89. Display mixed content - Il mixed content è una pagina Web o un e-mail che contiene elementi sicuri (https) insieme a elementi insicuri (http). Questo settaggio consente di rilevare per esempio se un e-mail contiene questa miscela e di chiedervi come mai: potrebbe esserci dietro un tentativo di truffa.
90. Il primo determina il modo in cui Windows gestisce l'autenticazione quando si accede a un sito che richiede nome utente e password: a A volte il logon viene fatto automaticamente usando nome e password di Windows. L'SCP controlla lo scaricamento automatico di software dai cosiddetti "channels" (siti accessibili tramite abbonamento).
91. In Eudora, Tools > Options > Viewing Mail. Disattivare Use Microsoft's Viewer, Show Message preview pane, Allow executables in HTML content.
92. www.microsoft.com/windows/ie_intl/it/iereadme.htm. "Quando l'opzione è selezionata, per i messaggi ricevuti in formato HTML verranno visualizzate solo le parti di testo normale, mentre le sezioni HTML verranno spostate in un allegato HTML, identificato dall'icona a forma di graffetta nel riquadro di anteprima o visualizzato nell'area degli allegati del messaggio aperto."
93. www.microsoft.com/security/incident/settings.mspx
94. Io l'ho fatto. L'imbeccata arriva dritta da Microsoft: www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2email.mspx. Un lettore (sandon) conferma il baco e segnala che non esiste in Windows 2000 SP4.
95. Prova personale: su un XP pre-SP2 privo di Word e del reader .DOC Microsoft, l'estensione DOC è bloccata. Idem per l'estensione PDF prima di installare Acrobat Reader. Dopo aver installato AcroReader, l'estensione PDF si è sbloccata senza dover neppure riavviare OE.
96. www.jmu.edu/computing/security/info/outlookav.shtml
97. Classico esempio: KAK-Worm, dicembre 1999, securityresponse.symantec.com/avcenter/venc/data/wscript.kakworm.html
98. support.microsoft.com/default.aspx?scid=kb;en-us;261255&sd=tech: ...allows a malicious Hypertext Markup Language (HTML) e-mail message to monitor the contents of the Outlook Express preview pane. After you view a malicious e-mail message in the preview pane, the contents of subsequent e-mail messages that you display in the preview pane can be sent to the malicious e-mail message's

author.

99. Sono stati scritti vari programmi, come Fidolook (www.fidolook.org), che permette di disabilitare script, activex e download; selezionando "force offline" impedisce anche il caricamento delle immagini remote (segnalazione di un lettore, non ho testato personalmente).
100. www.microsoft.com/windowsxp/using/web/sp2_oe.mspx
101. Post-SP2, l'estensione sxw di OpenOffice.org non viene più bloccata ma è accettata senza riserve.
102. Dettagli e lista estensioni bloccate: support.microsoft.com/?kbid=883260
103. www.hutteman.com/weblog/2003/12/28-151.html
104. Per maggiori informazioni sul problema del phishing: www.antiphishing.org; www.fraudwatchinternational.com/internetfraud/phishing.htm, /www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf
105. www.maxkava.com/spam/spam_intro.htm
106. È il caso di Phatbot: www.lurhq.com/phatbot.html
107. lists.netsys.com/pipermail/full-disclosure/2003-October/011339.html
108. www.spywareinfo.com/articles/p2p/
109. I miei revisori pignolissimi (e per questo preziosi) hanno segnalato più volte l'apparente errore della grafia *libriccino*, chiedendo di scriverlo con una C sola. Rispondo con il parere di Giorgio De Rienzo, linguista del Corriere della Sera (www.corriere.it/Rubriche/Scioglilingua/2003/29dicembre.shtml: "*Il diminutivo di libro è «libriccino» come ho letto sul «Corriere» o «libricino»? Bisogna affidarsi alla regola generale («cuoricino», «mattoncino») o costituisce un'eccezione? Il diminutivo di «libro» ha tutte le due forme, con una o due «c»*."
110. REFUSO: nella versione cartacea c'è scritto *i* al posto di *dei*.
111. Si può contenere il danno impostando una password per l'account Administrator. Riavviare il PC e premere F8 dopo il test fatto dal BIOS. Scegliere Safe Mode/Modalità provvisoria. Premere Invio nella schermata successiva. Una volta avviato Windows, andare nel Pannello di controllo, aprire Users Accounts, scegliere l'account Administrator e dargli una password. Poi riavviare il PC. (www.tweakxp.com/tweak1128.aspx)
112. È apparentemente disattivabile in Pannello di controllo > User accounts, ma in realtà non viene disattivato: viene nascosto ma resta attivo (per consentire le condivisioni) (www.petri.co.il/disable_the_guest_account_in_windows_xp.htm)
113. Per esempio, molti fabbricanti di computer includono una password "passepartout" che scavalca quella che impostate voi. Queste super-password non sono segrete; su Internet se ne trovano interi elenchi suddivisi per marca. In alternativa, si può togliere la batteria-tampone del BIOS, in modo da azzerare il BIOS, che così "dimentica" la password che avete impostato. Un altro metodo è smontare il computer, estrarne il disco rigido e montarlo su un altro computer. Dico queste cose non per insegnarvi a scassinare, ma per mostrarvi quanto sia più impegnativo rispetto al normale metodo

"infila un dischetto e sei dentro".

114. La password Supervisor serve per accedere alla configurazione del BIOS, ma in alcuni BIOS è necessario che sia abilitata (non vuota), altrimenti non è accessibile l'impostazione della password *User*.
115. Questo era un tempo (prima di Internet) la tecnica di diffusione più frequente dei virus. Oggi è rara, ma esistono ancora dei virus recenti che la sfruttano, per esempio Bacros (www.f-secure.com/v-descs/bacros_a.shtml).
116. Il salvaschermo è uno dei file con estensione SCR nella cartella system32 di Windows.
117. Rispettivamente in WMP 9 e in WMP 10.
118. support.microsoft.com/default.aspx?scid=kb;EN-US;290945
119. www.apogeonline.com/webzine/2003/07/30/01/200307300101
120. A tutto questo si aggiunge la spinosa questione del cosiddetto Unique Identifier di Word 97, un numero identificativo univoco che (dice Microsoft) consente a "strumenti di terze parti di lavorare con i documenti creati da Office e far riferimento ad essi". I maligni notano che siccome questo identificativo include il MAC address (identificativo univoco dell'eventuale scheda di rete presente nel PC), a dire il vero consente di sapere esattamente da quale computer (e quindi da chi) è stato scritto o modificato un qualsiasi documento Word. Grazie al cielo quest'informazione è stata rimossa dalle versioni successive del popolarissimo programma Microsoft.
121. www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360
122. www.f-secure.com/v-descs/bacros_a.shtml#details: When run via the registry with argument -t (MSDosdrv), the program drops a Word document infected with W97M/Bacros.A virus in two places: to user's personal documents folder and in %SystemRoot% folder with the name "WordInfo.doc". It also tries to disable the MS Office macro virus protection in the registry.
123. Settaggi sicuri di Word secondo documento NIST, p. 92.1. Open Microsoft Word. 2. Select Tools, then Macros, then Security. 3. Change the Security Level from High to Very High. This process should be repeated for each application in the Office 2003 suite, as this setting is not shared between the applications. The only difference is that the maximum Security Level in Publisher is High rather than Very High. One new feature of Office 2003 is the ability to collaborate with other people via a Shared Workspace or Share Point site. Unless this feature is needed, it should be disabled by performing the following steps: 1. Open Microsoft Word. 2. Select Tools, then Options. 3. Select the General tab and click the Service Options button. 4. Deselect the check boxes for The document is part of a workspace or SharePoint site and There is important status information regarding the document.
124. È possibile indurre Word a eseguirle lo stesso (www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-035.asp) a meno che l'utente installi una patch di correzione.

125. www.hexview.com/docs/20041006-1.txt
126. In Word 2000 UK, Tools > Options > Save > Embed TrueType fonts.
127. www.linuxsecurity.com/advisories/redhat_advisory-4701.html; seclists.org/lists/bugtraq/2004/Oct/0116.html
128. REFUSO: nella versione cartacea, manca questo *un*.