▶ Sicurezza

Spam, adware e spyware: conoscerli per evitarli

Le informazioni di base e una selezione dei migliori programmi per difendersi: MailWasher, Spam Punisher e Ad-Aware

di Michele Nasi

Nel linguaggio informatico e, più propriamente, in quello legato a Internet, si definisce *spam* tutta una serie di comportamenti che non sono conformi alla *netiquette* (una serie di semplici regole che tutti coloro che fanno uso di Internet è bene tengano a mente e rispettino al fine di una buona "convivenza" in Rete: www.nic.it/NA/netiquette. txt). Se cercate su un dizionario inglese la parola spam troverete qualcosa di simile: "carne suina in scatola". Il sostantivo spam deriva infatti da Spiced Pork Ham: si tratta delle famose scatolette che erano fornite in dotazione ai militari americani nel dopoguerra.

Nonostante il problema spam sia spesso associato, visivamente, ad una scatoletta di carne, i più fanno derivare il sostantivo spam da una scenetta di Monty Python nella quale un'allegra combriccola di commensali, travestiti da vichinghi, non fa altro che ripetere «spam, spam, spam…» alla cameriera, giunta per ritirare le ordinazioni. Così facendo, il loro frastuono non permette, ad una coppia di clienti, di capire cosa c'è nel menù (le parole della cameriera sono costantemente superate, per intensità, dalle urla dei vichinghi). Alla fine, la coppia non può far altro che ordinare spam…

Il termine spam, in ambito informatico, è stato scelto, quindi, per descrivere tutte quelle azioni che, in genere, ostacolano le proprie possibilità di comunicazione.

Avete presente quelle fastidiosissime e-mail pubblicitarie che spesso trovate nella vostra casella di posta elettronica? Solitamente trattasi, appunto, di spam poiché si ha a che fare con e-mail non richieste, contenenti materiale indesiderato: tali messaggi di posta non fanno altro che farci perdere tempo.

Uno studio fatto dalla Commissione Europea

Alcuni utenti ricevono molti messaggi indesiderati: talvolta si tratta di una ventina di e-mail al mese, altre volte possono superare il centinaio. Se poi si fa uso, da tanti anni, del medesimo indirizzo e-mail senza aver applicato alcuna attenzione a difesa dallo spam, è possibile veder arrivare, mensilmente, un numero di e-mail indesiderate ancora superiore.

Ci sembra interessante citare lo studio effettuato lo scorso anno per conto della Commissione Europea (http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamstudyen.pdf): leggendo il documento si evince, come conclusione, quale sia il danno economico causato dal fenomeno spam: si è calcolato che, per la comunità mondiale degli utenti collegati alla Rete Internet, scaricare i messaggi di spam costerebbe circa dieci miliardi di euro all'anno (circa 30 euro l'anno per ogni singolo utente). A questi costi vanno poi aggiunti quelli sostenuti dai provider Internet: spese che, alla fine, vanno a gravare sempre più sugli utenti.

Prevenire è meglio che curare

Coloro che effettuano *spamming* ossia che inviano e-mail pubblicitarie indesiderate ai quattro ovunque, fanno uso di speciali programmi che provvedono a "scandagliare" periodicamente la Rete alla ricerca di indirizzi e-mail comparsi nelle comuni pagine Web.

La cosa più importante da mettere in pratica suonerà un po' banale, in realtà è la chiave di volta che permette di evitare la ricezione di e-mail indesiderate: tenere riservato il proprio indirizzo e-mail.

Una volta infatti che tale indirizzo di posta elettronica viene scovato da parte di uno o più *spammer*, questo viene rivenduto ad altri spammer e poi ad altri ancora: vi ritroverete quindi tonnellate di spam nella casella di posta presa di mira.

Il consiglio migliore è quindi quello di evitare di rendere pubblico al mondo intero il vostro indirizzo di posta elettronica e di utilizzarlo solo per scambiare messaggi con colleghi, amici e parenti.

E per partecipare a newsgroup e forum, per pubblicare l'e-mail sul proprio sito Internet? Come fare?

La cosa più sensata è quella di creare un account di posta elettronica "di servizio" (per esempio tramite i tanti servizi gratuiti disponibili in Rete) che sia "sacrificabile" senza problemi qualora dovesse cadere nelle mani degli spammer. Così facendo, l'intento è quello di evitare la diffusione degli indirizzi e-mail più importanti come, ad esempio, quello aziendale.

L'indirizzo aziendale dovrebbe essere utilizzato solo per la corrispondenza con persone di fiducia e non dovrebbe mai essere reso disponibile sul Web.

In ogni caso, di qualunque indirizzo e-mail si disponga, è bene seguire una serie di semplici regole che permetteranno di evitare di essere bombardati da messaggi indesiderati.

Attenzione ai newsgroup

In Internet esistono migliaia di gruppi di discussione riguardanti gli argomenti più disparati: all'interno dei newsgroup è possibile scambiare messaggi con persone di tutto il mondo che condividono i medesimi interessi. I newsgroup, accessibili facendo uso dell'apposita funzione contenuta nel client di posta elettronica o da apposite interfacce rese disponibili sul Web (ad esempio http://groups.google.com o www.mailgate.it), sono anche la migliore fonte di indirizzi e-mail per gli spammer: i campi *from* e *reply to* contengono spesso indirizzi di posta elet-

Le regole per difendersi

1. Non "pubblicizzate" i vostri indirizzi e-mail personali: forniteli solo a persone di fiducia
2. Per partecipare a qualsiasi discussione in Rete (newsgroup, forum) o per la pubblicazione su siti Web usate indirizzi e-mail "sacrificabili"
3. Non rendete noto il vostro indirizzo e-mail neppure nelle chat
4. Evitate di porre il vostro indirizzo e-mail nella procedura di configurazione del browser Internet
5. Mascherate i vostri indirizzi e-mail quando scrivete sui newsgroup
6. Non rispondete mai alle e-mail indesiderate
7. Usate un software apposito per filtrare la posta e scartare i messaggi indesiderati
8. Se lo ritenete opportuno, protestate con il provider Internet che fornisce il servizio allo spammer

I newsgroup, *come ad esempio quelli che si trovano su Google, sono una delle migliori fonti di indirizzi e-mail per gli spammer*

tronica validi che gli spammer usano a piacimento.

Dal punto di vista dell'efficacia del messaggio pubblicitario, lo spammer può addirittura suddividere le diverse e-mail secondo il newsgroup all'interno del quale sono state reperite: in questo modo otterrà un elenco ripartito in base agli interessi dei vari utenti, rivendibile a caro prezzo.

Una soluzione per non ricevere posta indesiderata sarebbe quella di non specificare alcunché nei campi from e reply to: in questo modo, però, chi desiderasse contattarvi in privato, leggendo un vostro messaggio sui newsgroup, non potrà farlo.

Il consiglio è quello di mascherare il proprio indirizzo e-mail con un semplice ma efficace espediente.

All'atto della creazione di un nuovo account per la lettura dei newsgroup, digitate l'indirizzo e-mail "di servizio" che avete scelto in precedenza, quindi abbiate l'accortezza di modificarlo in modo da renderlo non più valido.

Supponiamo, ad esempio, che il vostro indirizzo e-mail sia mario.rossi@provider.it: dopo il simbolo @ provvedete ad inserire un termine tale da invalidare l'indirizzo. Nel nostro caso abbiamo scelto di inserire la frase "toglimiperrispondere" opportunamente evidenziata con caratteri maiuscoli.

Nel testo del messaggio che si invia al newsgroup è poi bene specificare le istruzioni per permettere agli interessati di rispondervi. Ad esempio, nel nostro caso, si dovrà spiegare brevemente che, per inviare un'e-mail, si dovrà rimuovere dal campo "destinatario" la frase "toglimiperrispondere".

Il perché di tutto questo? Gli spammer utilizzano software automatici per carpire nuovi indirizzi dai newsgroup: mascherando la propria e-mail con l'espediente suggerito, gli spammer invieranno la loro posta elettronica ad indirizzi inesistenti. Inesorabilmente, tutte le loro e-mail ritorneranno al mittente come un boomerang senza arrecarci alcun disturbo.

Non "falsificate" mai il vostro indirizzo e-mail come mario.rossi@NOSPAMprovider.it: i software usati dagli spammer sono sempre più evoluti e sono in grado di riconoscere ed eliminare i termini più diffusi per mascherare i propri indirizzi di posta. Usate quindi la fantasia: c'è chi nei suoi messaggi è giunto a scrivere "per rispondermi si prega di togliere il TAPPO dall'indirizzo e-mail" oppure "per contattarmi levate LEDITADALNASO" camuffando i propri indirizzi, rispettivamente, in mario.rossi@TAPPOprovider.it e mario.rossi@LEDITADALNASOprovider.it.

Il consiglio è poi quello di non apporre, neppure nel corpo del messaggio, i vostri indirizzi e-mail in chiaro.

Indirizzi pubblicati su siti Web personali

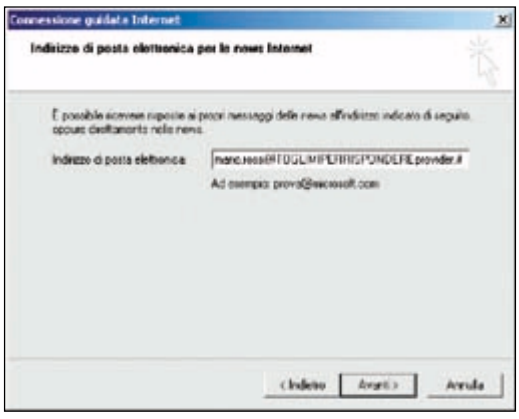
Per difendere un indirizzo e-mail pubblicato sul proprio sito Web, si può ricorrere ad un trucco assai efficace e di semplice realizzazione. Prelevate il programma AssMaker all'indirizzo http://assmaker.mybravenet.com, estraete il contenuto del file compresso all'interno di una cartella quindi eseguite il programma.

Inserite la prima parte del vostro indirizzo e-mail ossia ciò che precede la @ nella casella *Username*, ciò che segue nel campo *Domain 1* ed il suffisso *.it*, *.com*, *.net* o *.org* (presente in fondo ad ogni indirizzo e-mail) nella casella *Domain 2*. Cliccate quindi il pulsante ▷

"QUELLA SPORCA DOZZINA": LE 12 CATEGORIE DI SPAM

Nel luglio del 1998 la Federal Trade Commission americana (http://www.ftc.gov) ha pubblicato una lista delle 12 truffe più comuni messe in atto dagli spammer per carpire e-mail:

① Schemi piramidali, che promettono grandi ritorni per piccoli investimenti
② Truffe che promettono soldi facili se si diventa spammer e si vendono liste di indirizzi o di software per fare spamming. Le liste sono spesso di cattiva qualità e lo spamming di solito viola il contratto che le vittime hanno con il loro ISP
③ Catene di Sant'Antonio
④ Proposte di lavoro a casa retribuito, (come ad esempio,riempire buste o piccoli lavori manuali). Spesso le vittime non ricevono alcun compenso.
⑤ Truffe legate all'ambito della salute e delle diete.
⑥ Truffe legate allo scambio di valuta.
⑦ Truffe che promettono l'invio di merce gratuita in cambio del pagamento di un abbonamento; le vittime scoprono (dopo aver pagato l'abbonamento) che non sono qualificati per ricevere la merce finchè non portano altri abbonamenti.
⑧ False opportunità di investimento.
⑨ Offerte di kit pirata per TV via cavo che, se funzionano sono illegali, ma nella maggior parte dei casi non funzionano neppure.
⑩ Mutui per acquisto di immobili o carte di credito a credito illimitato che non si materializzeranno mai
⑪ Truffe che promettono la cancellazione dei debiti accumulati con la carta di credito a fronte di un pagamento. Negli Stati Uniti creare una nuova identità creditizia è illegale.
⑫ Offerte di vacanze premio, che offrono soggiorni da sogno a prezzi stracciati. Le vittime scoprono che le sistemazioni non sono proprio "lusso" a meno di sborsare un cospicuo extra.



Ecco due trucchi per evitare di far conoscere la vostra e-mail: *inserire dopo @ un termine che invalidi l'indirizzo, oppure specificare delle istruzioni per permettere agli interessati di rispondervi*

▷Make. AssMaker genererà un codice Javascript contenente il vostro indirizzo e-mail che difficilmente potrà essere intercettato dagli spider utilizzati da parte degli spammer.

Prima di chiudere AssMaker aprite la pagina HTML del vostro sito Web, all'interno della quale desiderate porre un riferimento al vostro indirizzo e-mail quindi scegliete dal menu*Modifica* la voce *Incolla*.

Un altro suggerimento utile è quello di scegliere indirizzi e-mail poco comuni. Molti spammer, oltre ad usare programmi in grado di "analizzare" le pagine Web e i newsgroup alla ricerca di indirizzi e-mail, fanno uso di software basati su un sistema di tipo *dictionary attack*. In pratica, si tratta di programmi in grado di generare indirizzi e-mail utilizzando combinazioni di termini più o meno diffusi (nomi, cognomi ed altre parole molto usati negli indirizzi di posta). Avete capito bene: gli spammer tirano anche ad indovinare.

Per difendersi abbiate cura di scegliere, per le vostre e-mail "di servizio", termini poco noti.

E la legge?

Non ci sono leggi che possano tutelare gli interessi degli utenti collegati ad Internet fornendo loro, pari tempo, uno strumento efficace per denunciare chi si rende colpevole di spam?

Va detto che pure negli Stati Uniti, Paese dal quale provengono la maggior parte di e-mail indesiderate, manca una legislazione specifica che tratti il problema dello spam.

Eppure una legge statunitense (US Code Title 47, Section 227: www.law.cornell.edu/uscode/47/227.html) ha già affrontato e risolto un problema simile: l'abuso del servizio fax a scopi pubblicitari.

Tale normativa, nota come junk fax law, punisce chi invia fax pubblicitari non richiesti: spedire via fax documenti non richiesti arreca danno all'azienda perché, potenzialmente, non le permette di ricevere altre comunicazioni importanti. "Convertire" tale normativa al mondo di Internet non è apparso facile.

Ecco allora che sono nate la CAUCE (*Cohalition Against Unsolicited Commercial Email*; www.cauce.org) insieme con altre iniziative come il F.R.E.E (www.spamfree.org).

Visitando il sito della CAUCE vi renderete conto di che cosa si stia muovendo intorno al fenomeno spam: vi accorgerete, ad esempio, di quali siano le proposte di legge valide per arginare lo spam imbattendovi in altre proposte, presentate da figure vicine agli spammer, tese a legalizzare l'invio di e-mail non richieste.

In Italia c'è essenzialmente il D.L. 185 del 22 Maggio 1999 che però né contiene la definizione di spam né analizza in modo dettagliato i comportamenti punibili.

Va evidenziato, comunque, come il nostro Paese ritenga inaccettabile, dal punto di vista legislativo, l'invio di comunicazioni non richieste: qualsiasi consumatore può sporgere denuncia, oltre alle possibilità di procedere d'ufficio.

Ricordiamo, inoltre, il pronunciamento in data 11 Gennaio 2001 da parte del Garante per la tutela dei dati personali a seguito delle segnalazioni giunte da molti utenti che avevano ricevuto e-mail contenenti informazioni di propaganda politica senza averne richiesto la ricezione: è stato dichiarato illegittimo prelevare indirizzi di posta elettronica (pur da aree a pubblico accesso quali siti Web e newsgroup) ed utilizzarli, per le proprie esigenze d'affari o di qualunque altro genere, senza il con-

Adware e spyware: cosa sono e perché possono essere pericolosi

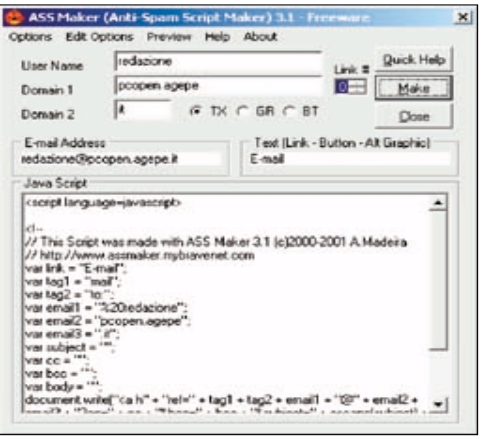
Internet offre programmi shareware e freeware di tutti i generi che, distribuiti in modo del tutto gratuito o quasi, permettono di soddisfare qualunque esigenza.
Certi programmi, però, nascondono al loro interno delle insidie: si tratta dei cosiddetti software *spyware* ossia di quei programmi che utilizzano particolari algoritmi che permettono di raccogliere informazioni sul nostro personal computer e sulle nostre abitudini e di trasmetterle, via Internet, a terze parti.
Molto spesso la raccolta e la trasmissione di dati personali avviene senza il nostro consenso: si tratta quindi di una pratica illegittima in Italia come in altri Paesi.
Il pericolo giunge dai software shareware e freeware che fanno uso della tecnologia adware ossia da gran parte delle applicazioni che, mentre sono in esecuzione, visualizzano banner pubblicitari.
Tali banner vengono, infatti, prelevati da un server che si occupa della loro gestione: è facile, quindi, intuire come si instauri, in questo caso, un collegamento diretto tra il nostro personal computer e un server Web che si occupa dell'esposizione di banner.
Le principali società che seguono lo sviluppo e la fornitura della tecnologia che permette la visualizzazione di banner pubblicitari all'interno di pacchetti software sono Radiate, Cydoor, Conducent, Web3000, Flyswat. Per evitare fraintendimenti, ci preme sottolineare come l'esposizione dei banner, di per sé stessa, non costituisca alcun problema né violi in alcun modo la privacy dell'utente.
Va sottolineato, poi, come alcuni software gratuiti o meno facciano uso di banner pubblicitari senza però adottare alcuna pratica lesiva nei confronti dell'utente. Non gridate quindi "al lupo, al lupo" non appena vi imbattete in un software che espone banner pubblicitari sin dalla prima esecuzione: seguendo i nostri consigli sarete in grado di evitare l'installazione di programmi potenzialmente pericolosi e di eliminare "le spie" eventualmente già presenti sul vostro personal computer.

Perché i software utilizzano questa tecnologia.

Le domande alle quali non abbiamo ancora risposto sono perché alcuni software che fanno uso della tecnologia adware possono essere pericolosi e perché gli autori di tali programmi hanno deciso di implementarla.
Diciamo subito che i software shareware e freeware, distribuiti gratuitamente via Internet, sono migliaia ma ben poche le persone che, a fronte di un esborso economico di solito abbastanza contenuto, si registrano presso gli autori acquistando una licenza d'uso personale.
Per ovviare a questo problema alcuni sviluppatori hanno deciso di fare uso della tecnologia adware messa a disposizione dalle società precedentemente citate: a fronte dell'esposizione di banner pubblicitari all'interno dei loro prodotti software, essi ricevono un compenso variabile che, qualora il proprio programma abbia successo su scala mondiale, possono portare a grandi guadagni.

Perché si tratta di una tecnologia potenzialmente pericolosa.

Il pericolo deriva dal fatto che, quando utilizziamo software adware, non possiamo sapere, in modo certo, quali dati vengono trasmessi durante la connessione Internet.
I programmi adware, in quanto tali, ricevono dati da un server Web (le informazioni riguardanti i banner pubblicitari che il programma deve esporre) ma



***Un trucco** efficace per difendere l'e-mail pubblicata su un sito è ricorrere al software AssMaker*

senso dei diretti interessati.

Liberare la casella di posta dalle e-mail non richieste

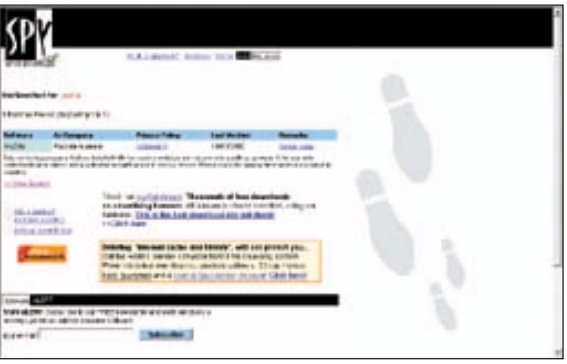
Alzi la mano chi non ha mai ricevuto nella propria casella di posta elettronica qualche esempio di spam. Pur applicando tutte le cautele del caso ed i suggerimenti poco fa presentati, col passare del tempo, immancabilmente, qualche indirizzo e-mail personale finisce per essere "catturato" da parte degli spammers.
Che fare? Per evitare di dover perdere tempo a scaricare "messaggi-spazzatura", è possibile adottare un software come **MailWasher** (contenuto nel CD ROM) che vi permetterà di controllare le intestazioni dei messaggi di posta elettronica presenti nella vostra casella prima ancora di scaricarli sul proprio personal computer.

Il programma fa uso di una serie di filtri, personalizzabili da parte dell'utente, che provvedono ad effettuare una scansione della posta elettronica quando questa risiede ancora presso il proprio Internet provider. MailWasher è in grado di riconoscere e marcare in modo opportuno le e-mail che con grande probabilità veicolano virus.

Passare alla controffensiva.

La principale arma per reprimere il fenomeno spam è la protesta che si dovrà rivolgere non, direttamente allo spammer dal quale si è ricevuto una o più e-mail indesiderate, ma al provider Internet che gli fornisce il servizio. Non rispondete mai ad un messaggio di spam: si tratta di un punto di importanza cruciale che va sempre tenuto a mente. Rispondendo, infatti, otterrete il solo scopo di confermare la validità del vostro indirizzo e-mail e continuerete a ricevere la fastidiosa posta. A qualunque computer collegato con la Rete Internet viene assegnato un indirizzo IP (ad esempio: 123.456.789.123) che ne rende possibile l'identificazione. Non è possibile conoscere qual è la persona fisica che sta dietro un determinato indirizzo IP però è relativamente semplice sapere quale provider gli fornisce il servizio per l'accesso ad Internet.

La prima cosa da fare per protestare con il provider Internet è controllare gli *header* (ossia l'intestazione dell'e-mail di spam) quindi verificare cosa compare accanto alle voci *Received*. A beneficio di tutti, anche dei meno esperti, presentiamo, nelle pagine successive, **Spam Punisher**, (contenuto anche nel nostro CD ROM) un programma che provvede a preparare, in modo automatico, un'e-mail di protesta da spedire al provider Internet che fornisce l'accesso allo spammer. L'e-mail viene spedita attraverso il client di posta elettronica predefinito e può essere personalizzata a piacimento da parte dell'utente prima dell'invio. ■



come possiamo essere certi che la comunicazione avvenga solo in questa direzione e non vi sia, quindi, anche una trasmissione di informazioni dal nostro computer verso la rete Internet?
È proprio questa la differenza che distingue i software adware dagli spyware. Mentre i primi si limitano esclusivamente a ricevere informazioni da Internet in modo da visualizzare banner pubblicitari, i secondi inviano spesso anche dati relativi alla nostra identità, alle nostre abitudini, alle informazioni memorizzate sul personal computer.
Si pensi, per esempio, a quali e quante informazioni siano memorizzate all'interno del registro di sistema di Windows: codici di registrazione di software con il nostro nome e cognome in chiaro, username e password per la connessione ad Internet e tanti altri dati relativi alle applicazioni installate ed alla configurazione del sistema. Operazione assai semplice risulterebbe per un programma recuperare questi dati e ritrasmetterli altrove attraverso la Rete.
Ovviamente i programmi spyware che si comportano in modo "sconsiderato" sono davvero pochi: le software house produttrici dovrebbero sostenere cause legali già perse in partenza e perderebbero tutta la loro credibilità.

Eliminazione delle "spie" con Ad-Aware.

Per evitare ogni tipo di problema, esistono particolari software che, effettuando una scansione completa del personal computer, sono in grado di trovare ed eliminare tutti gli eventuali componentiadware e spyware facenti parte dei programmi installati.
Il programma migliore che agisce in tal senso si chiama **Ad-Aware** ed è distribuito in maniera del tutto gratuita da Lavasoft, una piccola software-house tedesca: lo analizziamo a pagina 37 e lo trovate contenuto nel CD ROM allegato alla rivista *(categoria Internet).*

Altri metodi per accorgersi della presenza di spyware: i firewall.

A patto che venga tenuto costantemente aggiornato mediante l'installazione dei reference file più recenti (gli archivi contenenti informazioni sugli adware/spyware), Ad-Aware è certamente lo strumento migliore per diagnosticare ed eliminare le "spie" eventualmente presenti nel nostro personal computer.
Esistono, tuttavia, altri due metodi per accorgersi della presenza di spyware. Per prima cosa, alcuni di essi, durante la loro esecuzione "silenziosa", causano errori di protezione, ad esempio, all'interno del browser Internet (Internet Explorer o Netscape Navigator). Si tratta di errori, ad una prima analisi, inspiegabili e del tutto inattesi.
Con il passare del tempo però, anche gli spyware si sono evoluti ed i "campanelli di allarme" rappresentati da errori generali oggi si vedono sempre meno.
I software firewall, invece, rappresentano probabilmente, dopo Ad-Aware, i migliori nostri alleati nello scovare tentativi di comunicazione con la Rete da parte di componenti adware e spyware.
Anche noi abbiamo scovato l'attività effettuata a nostra insaputa da spyware: il firewall, una volta attivato, informa l'utente su tutti i tentativi di accesso ad Internet da parte delle applicazioni installate.
Come vi abbiamo suggerito negli articoli sull'argomento apparsi nei numeri precedenti di *PC Open*, il nostro consiglio è quello di negare l'autorizzazione a comunicare con la Rete Internet ai programmi che non si conoscono: si avrà il tempo per rendersi conto dell'accaduto.

Una lista di software spyware.

Su Internet sono pubblicate e costantemente aggiornate delle liste che permettono di rendersi conto di quali programmi contengano spyware. Un primo esempio di lista è consultabile all'indirizzo www.tom-cat.com/spybase/spylist.html.
Prima di scaricare un nuovo software shareware/freeware dalla Rete, una buona idea è quella di fare riferimento all'indirizzo www.spychecker.com.
Indicando, nell'apposita casella di ricerca che campeggia in home page, il nome del programma che intendete installare: scoprirete se tale software fa uso di componenti spyware.

▶ MailWasher

Prevenire è meglio che curare

MailWasher è un programma estremamente utile che permette di controllare le intestazioni dei messaggi ed eliminare dalle proprie caselle di posta elettronica tutta la "spazzatura" presente, prima ancora che venga scaricata sul vostro personal computer.

Il programma, infatti, si collega all'Internet Service Provider ove risiedono le nostre mailbox quindi si incarica di verificare il contenuto di ciascuna casella di posta riconoscendo, in modo automatico, messaggi di spam e virus.

MailWasher include, infatti, al suo interno un evoluto filtro anti-spam che consta di un'ampia raccolta di informazioni circa tutti i più diffusi esempi di spam via Internet.

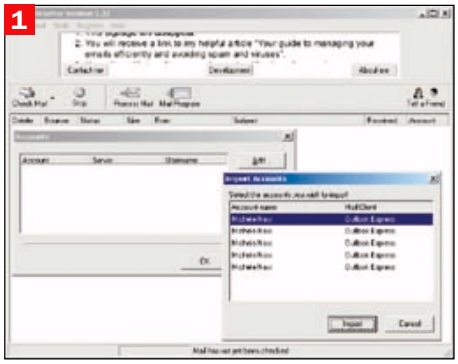
Per ciascun messaggio presente in mailbox, MailWasher ne evidenzia chiaramente il contenuto indicando le e-mail sospette.

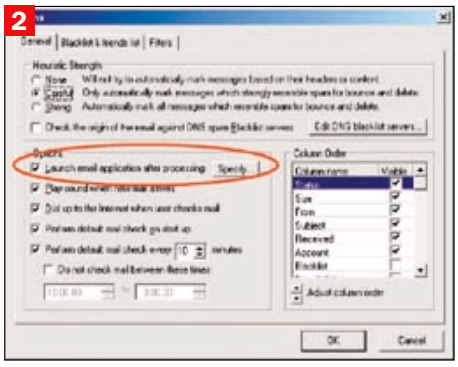
Si tratta di un software che permette di evitare infezioni da virus worm, sempre più diffusi attraverso la posta elettronica. Pur non sostituendosi assolutamente all'antivirus (che è sempre bene installare e mantenere costantemente aggiornato), MailWasher è in grado di riconoscere molti virus diffusi via e-mail sfruttando il fatto che molte tipologie di worm si presentano con messaggi dalle caratteristiche abbastanza simili.

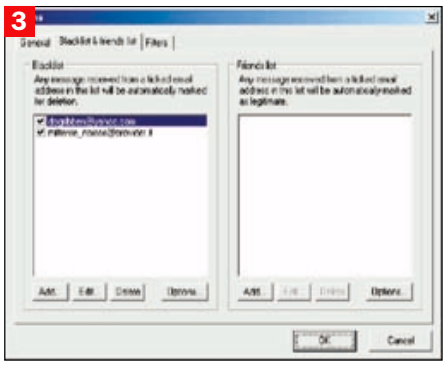
Poiché molti virus "agganciano" alla e-mail pesanti allegati (di dimensioni, spesso, davvero notevoli) MailWasher permette di eliminare tali messaggi direttamente alla fonte senza doverli scaricare sul proprio personal computer: in questo modo sarete in grado di risparmiare tempo e denaro.

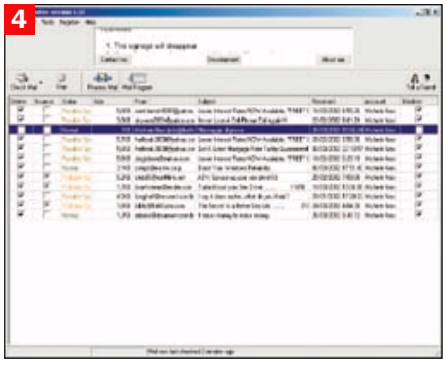
MailWasher è distribuito in forma completamente gratuita (www.mailwasher.net): registrandosi, tuttavia, si gratificherà l'autore e si eliminerà il banner visualizzato nella finestra principale (ricordiamo, comunque, che il programma non fa uso di spyware). n

Come evitare la "spazzatura" in quattro mosse









1 La prima volta che MailWasher viene avviato, il programma mostra una finestra mediante la quale è possibile specificare l'elenco dei propri account di posta elettronica utilizzati. Cliccando sul pulsante *Add* si potrà specificare i dati necessari per l'accesso ad ogni singola casella di posta (nome account, server POP3, server SMTP, username e password). Nella stragrande maggioranza dei casi, in alternativa, qualora si abbia già installato e configurato un programma per la gestione della posta elettronica (come Outlook Express), basterà premere il pulsante *Import* per importare i dati per l'accesso ai propri account di posta.

2 Una volta importati o configurati i parametri necessari per l'accesso ai propri account di posta, MailWasher è già pronto per passare all'azione. Vi consigliamo tuttavia di dare uno sguardo anche al menu *Tools, Options* che offre una serie di interessanti possibilità. In primo luogo MailWasher permette di specificare quale client di posta (ad esempio Outlook Express o Eudora) deve essere eseguito dopo il controllo dei messaggi di posta (opzione *Launch email application after processing*); consente poi di specificare le proprie preferenze relative all'operazione di analisi automatica della posta (numero di minuti tra un controllo e l'altro; fasce orarie escluse).
Dalla lista *Column order*, vi consigliamo di rendere visibile anche la colonna *Blacklist*.

3 Tra le altre possibilità, ricordiamo l'opzione che permette di controllare i mittenti delle varie e-mail e di ricercarli all'interno dei database anti-spam (*Check the origin of the email against DNS spam Blacklist servers*). Attivando questa opzione, il programma avrà un'arma in più per riconoscere, senza ombra di dubbio, i messaggi contenenti spam.
L'opzione, qualora venga attivata, rallenta però un poco il processo di controllo delle e-mail. La scheda *Blacklist & friends list* permette di specificare due elenchi di indirizzi e-mail: il primo, con lo scopo di marcare come da eliminare tutti i messaggi provenienti dai mittenti specificati (*blacklist*); il secondo, per visualizzare come attendibili tutti quelli che giungono da mittenti amici (*friends list*).

4 Per avviare il controllo delle caselle di posta configurate, basta cliccare *Check mail*. Nella finestra principale verranno elencate le intestazioni di tutti i messaggi presenti quindi verranno evidenziati i messaggi contenenti spam o virus. Mettete il segno di spunta sulla casella *Delete* corrispondente ai messaggi che volete vengano cancellati dal server. Spuntate anche la casella *Blacklist* se desiderate, d'ora in poi, che i messaggi provenienti dallo stesso mittente vengano automaticamente eliminati da parte di MailWasher. Premete, infine, il pulsante *Process mail* per sbarazzarvi dei messaggi indesiderati.

sul CD n. 60 PC Open

▶ Spam Punisher

Il giustiziere dell'e-mail

Con lo scopo di informare chi di dovere dell'accaduto, Spam Punisher è un programma che offre a chiunque la possibilità di contattare il provider Internet i cui servizi sono utilizzati dallo spammer per inviare le sue e-mail.

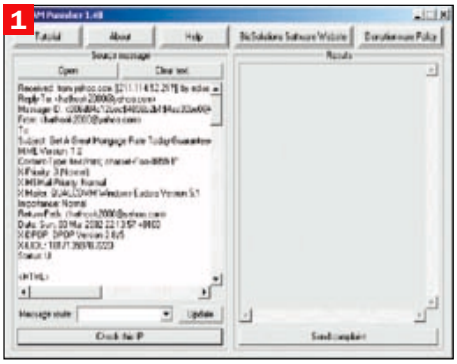
Non appena il provider Internet riceve la segnalazione preparata mediante l'uso di Spam Punisher, solitamente impedisce allo spammer di utilizzare ulteriormente i propri servizi.

Il funzionamento di Spam Punisher è abbastanza semplice: non appena si è individuato il messaggio di spam che si intende segnalare al provider Internet, è sufficiente incollare in un'apposita casella, il testo completo (compresi gli header: è importantissimo!).

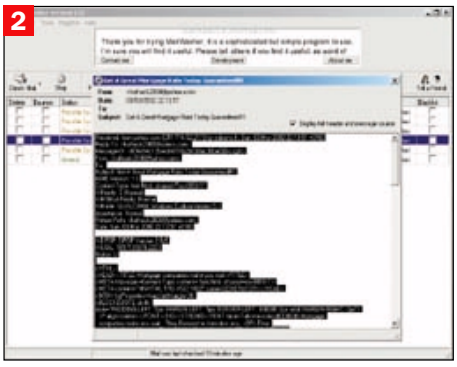
Non appena il provider Internet riceverà l'e-mail preparata con Spam Punisher, di solito (come spieghiamo a lato) prenderà dei provvedimenti nei confronti dello spammer.

Può accadere, talvolta, che il provider Internet contattato via e-mail mediante Spam Punisher, risponda di non essere in alcun modo responsabile per l'esempio di spam segnalato. Ciò può succedere quando lo spammer ha falsificato alcuni dei campi *Received* presenti nell'intestazione dell'e-mail. In questo caso vi suggeriamo di inviare l'e-mail di segnalazione all'Internet Provider immediatamente successivo: dal menù a tendina *Message Route* di Spam Punisher selezionate il secondo indirizzo IP, cliccate su *Check this IP* quindi sul pulsante *Send compliant*. Controllate sempre l'intestazione dell'e-mail: il primo dei campi *Received* indicherà il server del nostro provider Internet che ha ricevuto l'e-mail; gli altri *Received*, il percorso che ha compiuto l'e-mail prima di giungere a destinazione. I campi Received vi consentiranno di capire da dove è partito il messaggio. Tenete presente che gli indirizzi IP possono contenere cifre da 0 a 255: se vedete in un campo *Received* un indirizzo IP come 185.456.212.500 si tratta certamente di un campo falsificato da parte dello spammer. n

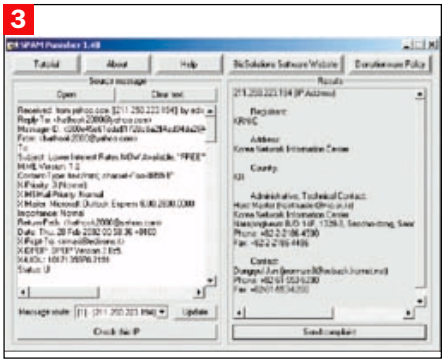
I passi per avvertire il provider



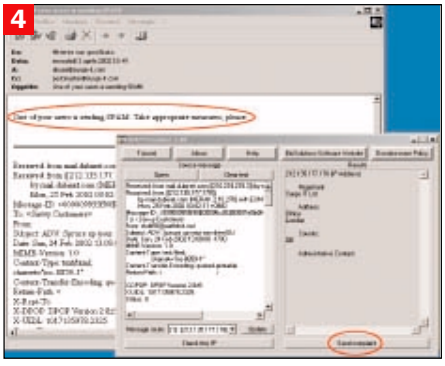
1 Per prima cosa individuate, tramite il vostro client di posta elettronica, il messaggio di spam che desiderate segnalare all'Internet Provider, quindi fate in modo di visualizzare il messaggio completo di *header* (intestazione). Nel caso in cui utilizziate Outlook Express fate clic con il tasto destro sul messaggio di spam, selezionate la voce *Proprietà*, cliccate sulla scheda *Dettagli* infine sul pulsante *Messaggio originale*. Selezionate l'intero messaggio (di solito inizia con il termine *Received*) usando la combinazione di tasti *CTRL+A*, premete quindi i tasti *CTRL+C* per copiare il tutto nell'area degli *Appunti di Windows*, cliccate sulla finestra *Source message* di Spam Punisher e premete *CTRL+V*.



2 Anche Spam Punisher consente di visualizzare i messaggi completi di header: selezionate il messaggio "incriminato", fate clic con il tasto destro su di esso, cliccate sulla voce *Preview message* infine spuntate la casella *Display full header and message source*. Evidenziate anche in questo caso l'intero messaggio usando *CTRL+A* quindi premete la combinazione di tasti *CTRL+C* per copiare l'intera e-mail nell'area degli Appunti di Windows; aprite Spam Punisher, selezionate il box *Souce message* quindi premete *CTRL+V*.



3 A questo punto, premete il pulsante *Update*, collocato nella finestra principale di Spam Punisher: il programma provvederà ad estrarre l'indirizzo IP utilizzato da parte dello spammer per l'invio dell'e-mail. Cliccate, quindi, sul pulsante *Check this IP* (Controlla questo indirizzo IP) per verificare a quale provider Internet appartiene l'indirizzo IP usato dallo spammer.
Dopo qualche secondo di attesa, otterrete nella finestra *Results* i dati relativi all'Internet Provider sfruttato da parte dello spammer.



4 Cliccando sul pulsante *Send compliant*, Spam Punisher aprirà il client di posta elettronica predefinito e creerà un nuovo messaggio di posta elettronica, pronto da spedire all'Internet Provider, contenente una copia del messaggio di spam da voi ricevuto. A questo punto si può spedire l'e-mail.
Solitamente, quando il provider riceverà la vostra segnalazione, provvederà a controllare che l'e-mail di spam sia stata effettivamente inviata attraverso il suo sistema di posta. In caso affermativo viene impedito allo spammer di utilizzare ulteriormente le risorse dell'Internet Provider (tranne alcune rare eccezioni i provider Internet non supportano lo spam).

▶ Ad-Aware

Per scovare adware e spyware

Ad-Aware è un programma gratuito (contenuto nel CD ROM guida di Pc Open) che consente di eliminare in pochi clic tutti gli eventuali componenti adware e spyware presenti sul sistema e facenti parte dei programmi shareware e freeware installati.

Il programma svolge un'indagine approfondita esaminando non solo i file memorizzati sui dischi fissi, ma anche ricercando possibili chiavi sospette all'interno del registro di sistema di Windows.

Va comunque tenuto a mente che alcuni programmi, una volta che si rimuovono le loro componenti adware o spyware non funzionano più.

Altri programmi, invece, continuano a funzionare senza problemi (addirittura senza visualizzare più banner pubblicitari durante la loro esecuzione) poiché, generalmente, le componenti adware o spyware sono delle unità operative esterne al programma vero e proprio.

Ad-Aware è compatibile con tutte le versioni di Windows, tuttavia, per eseguirlo in ambiente Windows NT 4.0/2000/XP ci si dovrà accertare di accedere al sistema con i diritti di amministratore.

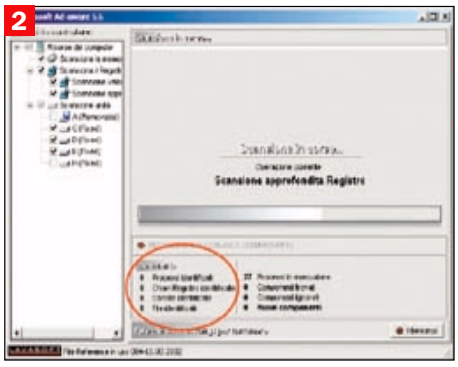
È consigliabile, inoltre, eseguire il programma immediatamente dopo il riavvio del personal computer verificando di non essere collegati ad Internet e provvedendo a chiudere quante più applicazioni possibile (anche quelle residenti in memoria).

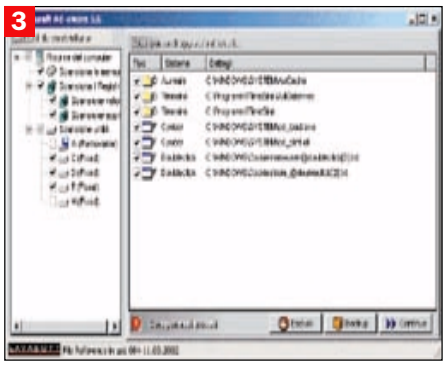
Così facendo il controllo diagnostico effettuato da Ad-Aware non verrà in alcun modo intralciato dalle applicazioni in esecuzione.

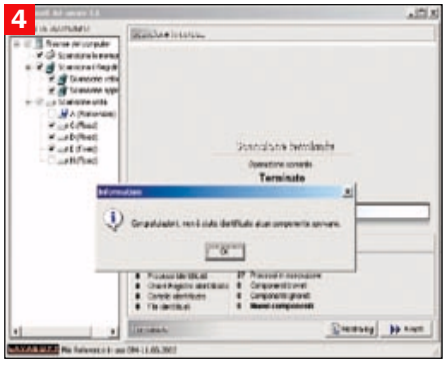
Da ultimo una raccomandazione: come tanti altri software Ad-Aware deve essere mantenuto aggiornato.

Affinché sia in grado di riconoscere ed eliminare tutti gli adware/spyware, si deve provvedere ad aggiornare, periodicamente, il cosiddetto reference file (ossia il file contenente informazioni su tutti gli adware/spyware conosciuti). ■

Come effettuare l'analisi ed eliminare gli intrusi







1 Terminata l'installazione, Ad-Aware si presenta come in figura. Per "tradurre" il programma in lingua italiana fate clic sul pulsante *Configuration* (Opzioni) quindi sulla scheda *Options* (Opzioni) e scegliete dal menù a tendina *Language* (Lingua) la voce Italiano quindi cliccate sul pulsante *Proceed* (OK).
In calce alla finestra principale trovate la versione del reference file (contenente tutte le informazioni su adware e spyware) attualmente utilizzato da parte del programma: verificate sul sito di Ad-Aware (www.lavasoftusa.com), la disponibilità di nuovi file di aggiornamento.
Per installare un nuovo reference file è sufficiente scaricarne l'archivio zip compresso quindi estrarne il contenuto nella cartella all'interno della quale è stato installato Ad-Aware.

2 La finestra a sinistra (*Sezioni da controllare*) consente all'utente di scegliere quali elementi del proprio sistema devono essere posti sotto la lente. Il nostro consiglio è quello di lasciare le impostazioni di Ad-Aware così come sono verificando, comunque, attraverso le caselle selezionate, che il programma effettui una scansione della memoria, un controllo veloce ed uno approfondito sul registro di sistema ed una scansione di tutte le unità disco installate.
Per avviare la procedura di scansione dei dischi fissi e del registro di sistema alla ricerca di componenti adware e spyware, basta cliccare sul pulsante *Scansiona*. Ad-Aware provvederà ad effettuare un'analisi approfondita informandovi passo-passo sul numero dei componenti sospetti che sono stati identificati.

3 Una volta concluso il processo di scansione è sufficiente premere il pulsante *Avanti per continuare*. Nel caso in cui Ad-Aware abbia trovato delle componenti adware/spyware, presenterà un elenco completo indicando file, cartelle e chiavi del registro di sistema sospetti.
Per fare pulizia ed eliminare tutti i componenti trovati, attivate le caselle corrispondenti apponendo l'apposito contrassegno di spunta.
Ribadiamo, comunque, che alcune applicazioni che fanno uso di componenti AdWare/spyware potrebbero non funzionare dopo la rimozione.
Per effettuare la pulizia premete il pulsante *Avanti*.

4 Una volta conclusa l'operazione, vi consigliamo di eseguire nuovamente una scansione completa del sistema così da accertarvi che tutti i file sospetti siano stati effettivamente eliminati: eseguite nuovamente Ad-Aware, cliccate sul pulsante *Scansiona* ed attendete il responso.
Se vi sarete sbarazzati di tutti i componenti adware/spyware, Ad-Aware si congratulerà con voi mostrando il messaggio in figura.

sul CD n. 60 PC Open