

SOMMARIO

146 **In prova**
6 prodotti scelti da CHIP

154 **Evitare la posta indesiderata**
Basta spam!

internet & networking

Lan Adapter • Devolo MicroLink dLan

Una Lan elettrica

Devolo presenta il MicroLink dLan, un adattatore che consente di realizzare una Lan sfruttando la linea elettrica domestica. *Di Andrea Pogliaghi*

■ L'idea di sfruttare la linea elettrica come mezzo di trasmissione dati è nata tempo fa e ha subito catturato l'attenzione dei fornitori di energia nazionali. Questo non sorprende più di tanto, se si considerano le enormi potenzialità di una simile tecnologia, che permetterebbe, per esempio, di offrire un collegamento Internet a ogni calcolatore connesso all'alimentazione, sfruttando un'infrastruttura preesistente a diffusione capillare come la linea elettrica, senza costi aggiuntivi.

Per evitare la proliferazione incontrollata di standard proprietari diversi e incompatibili, è stata fondata la HomePlug Alliance, un'associazione di produttori (tra cui figurano nomi del calibro di Panasonic, Motorola e Sony) che partecipano su base volontaria. Lo scopo di tale alleanza è quello di definire uno standard comune per la trasmissione di dati su linea elettrica, che i produttori membri si impegnano a rispet-

tare nella progettazione dei propri prodotti. La tedesca Devolo, azienda piuttosto giovane specializzata nella progettazione di sistemi di networking domestici e aziendali, ha recentemente presentato il MicroLink dLan (acronimo di Direct Lan, collegamento in rete diretto), un adattatore da inserire nella presa di corrente di casa che consente di utilizzare l'impianto elettrico in guisa di cavi di rete tradizionali.

Massima compatibilità

Il MicroLink dLan di Devolo garantisce la massima compatibilità essendo conforme agli standard di HomePlug. Il protocollo di trasmissione è basato sulla PowerPacket Technology di Intellon (riconosciuta da HomePlug Alliance), la quale implementa una versione evoluta della Ofdm (Orthogonal Frequency Division Multiplexing) dotata di controllo preventivo degli errori di ricezione, una tec-

nologia molto simile a quella adottata dai modem Dsl. Più in dettaglio, la banda di frequenze disponibili nel sottosistema elettrico (dai 4,3 MHz ai 20,9 MHz) viene suddivisa in 84 portanti tra loro ortogonali e i dati vengono spezzati in pacchetti di dimensione prefissata, quindi inviati simultaneamente su diverse portanti. Quando un disturbo sulla linea interferisce con una delle frequenze di trasmissione, i dati vengono indirizzati su diverse portanti: in questo modo si riesce a mantenere una connessione di classe Ethernet lungo la linea elettrica senza perdite di informazioni. Tale tecnica, inoltre, consente di limitare i disturbi provocati dall'inserimento di carichi sulla linea e attenuare gli effetti della degra-

busto, in grado di fornire un livello di protezione più che adeguato. Inoltre, le scelte progettuali di Devolo rendono ancora più difficile l'eventuale forzatura dell'algoritmo: la chiave condivisa è memorizzata all'interno di un chip posto all'interno dell'hardware e i dati vengono inviati all'interfaccia host solo dopo essere stati decrittati.

Facile installazione

L'installazione del MicroLink dLan avviene senza particolari problemi: per la versione Usb del dispositivo è sufficiente collegare il dispositivo al computer e inserire il Cd dei driver perché questo venga automaticamente rilevato; la versione Ethernet non necessita invece di alcun accorgimen-

gnale sono sensibili alla distanza, Devolo consiglia di non porre i dispositivi a più di 200 metri, anche se realisticamente 50-60 metri sono la soglia massima entro la quale le prestazioni si mantengono accettabili. Anche il numero di dispositivi contemporaneamente connessi impatta sulle prestazioni del dispositivo e, sebbene la tecnologia sia in grado di gestire un numero massimo di 253, Devolo sconsiglia di superare le 10 unità.

Il principale punto di forza del prodotto è legato alla versatilità di utilizzo, che consente di realizzare Lan o condividere l'accesso a Internet senza difficoltà in tutti i luoghi in cui sarebbe sconveniente realizzare una cablatura.

La tecnologia HomePlug, benché non offra la stessa mobilità di un collegamento wireless, resta comunque un'alternativa valida, soprattutto in virtù della banda garantita e della sicurezza delle trasmissioni. I MicroLink dLan di Devolo sono proposti sia in versione Ethernet sia in versione Usb, ma mentre la prima è utilizzabile indifferentemente con qualsiasi sistema operativo (non necessitando di driver), la seconda richiede necessariamente Windows. Sono infine presenti in commercio i cosiddetti starter kit, che contengono due dispositivi e permettono di realizzare una piccola rete locale.



Due versioni dell'adattatore: il modello con connettore Rj-45 è indipendente dalla piattaforma

dazione del segnale, eventualmente causati da impianti elettrici obsoleti.

Un problema importante, intrinseco all'utilizzo della linea elettrica come mezzo di trasporto dati, è senza dubbio quello della sicurezza. In primo luogo perché non è sempre semplice delimitare i confini dell'impianto elettrico al quale sono stati collegati i dispositivi, e in seconda battuta perché i dati potrebbero essere inviati per induzione anche su reti adiacenti, permettendo a utenti non autorizzati di accedere alle proprie informazioni. Devolo afferma che il contatore elettrico è generalmente un buon filtro, ma non garantisce la sua totale efficacia e consiglia pertanto di abilitare il sistema di crittografia a chiave condivisa Des a 56 bit implementato nei dispositivi. Si tratta di un algoritmo decisamente ro-

to. La realizzazione di una Lan o la condivisione di un accesso a Internet sono semplificati da un'utility fornita a corredo, che permette tra l'altro di attivare la crittografia impostando una chiave. Prima di avviare tale utility è bene premunirsi dei codici di sicurezza dei dispositivi che si intendono collocare nella rete, giacché questi verranno chiesti all'atto della configurazione. Sul fronte delle prestazioni, la tecnologia HomePlug è in grado di gestire fino a 14 Mbps di throughput ma, secondo Devolo, un MicroLink dLan installato in un rete elettrica in condizioni ottimali, dovrebbe garantire una velocità di collegamento fino a 6 Mbps. Si tratta di un valore comunque elevato, che rende il prodotto di Devolo una valida alternativa a soluzioni wireless. Poiché la velocità di trasmissione e la degradazione del se-

Devolo MicroLink dLan

QUALITÀ COMPLESSIVA

PREZZO/PRESTAZIONI

I giudizi di CHIP sono illustrati a pag. 240

- Versatilità
- Prezzo interessante
- Compatibilità limitata a sistemi Windows per la versione Usb

CHIP VI DICE CHE

Il MicroLink dLan consente di realizzare reti locali e condividere l'accesso a Internet bypassando il problema della cablatura

Tipo: adattatore Ethernet/cavo elettrico
Interfaccia: Ethernet (Rj-45) o Usb 2.0
Produttore: Devolo, www.devolo.it
Distributore: Euro Gate, tel. 02/84742243
Prezzo: euro 174,90

In prova

Switch • Longshine LCS-883R-SW2400

Massima versatilità

Lo switch per rete locale Fast Ethernet 10/100 di Longshine ha un buffer molto capiente ed è configurabile per la gestione delle reti Virtual Lan

■ Grazie alla larghezza standard di 19 pollici e alle alette per il montaggio in rack fornite in dotazione, lo switch Longshine LCS-883R-SW2400 si trova perfettamente a suo agio negli armadi di commutazione per cablaggio strutturato, ma può essere semplicemente appoggiato su un ripiano libero. Non è invece possibile appenderlo al muro, poiché le due piccole ventole di raffreddamento poste

centro le 24 porte Fast Ethernet 10/100 e quella di uplink; a destra si trova il connettore seriale Rs-232 per la programmazione facoltativa.

La posizione di spie e connettori è studiata per facilitare l'abbinamento con gli apparecchi da armadio dati dei principali costruttori mondiali. Uno sguardo all'interno del contenitore, facilmente accessibile per semplificare le ope-

Lan (Vlan) e del port trunking a quattro vie, supporto Nway per tutte le porte (che quindi negoziano in modo indipendente velocità e modalità half oppure full duplex).

A queste funzionalità evolute, che giustificano una buona velocità operativa anche in reti congestionate, fanno da contrappeso alcune limitazioni che tradiscono la tecnologia non proprio allo stato dell'ar-

di analisi dei guasti con le spie luminose. Nella maggior parte delle reti di piccole dimensioni queste funzionalità sono comunque superflue e quindi lo switch può essere messo subito in funzione, così come esce dall'imballo. Il manuale con le istruzioni per la configurazione è disponibile solo in lingua inglese.

La prova sul campo ha verificato il buon funzionamento dello switch, che grazie ai 3 Mb di buffer regge il confronto in prestazioni con apparecchi ben più costosi. Le funzionalità Vlan rudimentali, la tabella MAC ridotta, l'assenza di diagnostica in layer 3 e la mancanza delle segnalazioni di blocco ventole confinano però il Longshine LCS-883R-SW2400 all'uso su piccole reti, o come switch periferico.

Paolo Canali

Il case dello switch Longshine è di larghezza standard da 19 pollici: può essere installato in un armadio rack di commutazione o appoggiato su una scrivania

riori non riuscirebbero a raffreddare i circuiti interni, che occupano tutto lo spazio disponibile all'interno del robusto contenitore di lamiera metallica nera.

Accanto alle ventole, il pannello posteriore ospita la presa di alimentazione a 230 V, l'interruttore di alimentazione e il coperchio per il modulo opzionale 100Base-FX, su cui è possibile innestare una connessione a fibra ottica.

Il pannello frontale segue un'impostazione tradizionale: nella parte sinistra si trovano le spie di attività e i pulsanti di reset e di selezione della modalità di gestione delle spie; al

razioni di assistenza tecnica e la sostituzione del fusibile di protezione dell'alimentatore, rivela un cablaggio ordinato basato su una sola scheda logica che ospita sei chip Altima 0150TT, tre processori Allayer AL101, tre memorie da 512 Kword a 32 bit e un chip firmware su zoccolo, facilmente sostituibile in caso di aggiornamenti.

Specifiche di buon livello

Le scelte fatte da Longshine garantiscono caratteristiche tecniche più che rispettabili: 3 Mb di memoria per i pacchetti (gestiti con logica store-and-forward), gestione delle Virtual

te: la tabella degli indirizzi MAC ha appena 1.024 posizioni e la configurazione Vlan può avvenire solamente fuori banda, cioè collegando un terminale VT100 o un pc in emulazione terminale alla presa seriale sul pannello frontale, usando il cavo in dotazione. Il semplice menù testuale di configurazione segue le convenzioni ormai consolidate sulla maggioranza dei prodotti di origine orientale e, quindi, permette al sistemista esperto una veloce configurazione delle Vlan e del port trunking.

Non sono presenti funzioni diagnostiche o statistiche, eccetto una limitata possibilità

Longshine LCS-883R-SW2400

QUALITÀ COMPLESSIVA PREZZO/PRESTAZIONI

I giudizi di CHIP sono illustrati a pag. 240

 Funzioni Vlan e port trunking, buffer capiente **Costruzione solida** **Tabella MAC poco capiente** **Configurabile solo da console seriale**

CHIP VI DICE CHE

Nettamente più veloce e versatile di uno switch tradizionale, può sostituire vantaggiosamente i vecchi e lenti hub di rete locale

Porte: 24 Fast Ethernet 10/100, 1 Uplink 10/100, 1 Console Rs-232

Memoria per i pacchetti: 3 Mb

Tabella MAC: 1.024 indirizzi

Produttore: Longshine,

www.longshine.de

Distributore: Net.Com Italia,

tel. 06/35404007

Prezzo: euro 245,00

In prova

Broadband router • Unex NexIP IS050s

Banda larga condivisa

Lo switch di Unex è ideale per costruire piccole Lan e condividere una connessione broadband

■ L'IS050s di Unex è racchiuso in un guscio plastico nero e si presenta con una forma esteriore vagamente simile a quella di un comune modem esterno, ma con dimensioni leggermente superiori. Il dispositivo è dotato di quattro porte Fast Ethernet autosensing e da una porta Wan (Wide Area Network), anch'essa a 10/100 Mbps. Il di-

utente esterno di accedere a servizi in esecuzione sulle macchine protette dal firewall. Anche la sezione di Sicurezza è ben curata: sono da citare le possibilità di ignorare i ping in arrivo dal lato Wan, effettuare il mapping dei MAC address e adottare politiche di client filtering e restringere in questo modo gli accessi da e verso le porte dell'unità. Per quanto riguarda l'area di routing, l'IS050s offre la possibilità di impostare tabelle di routing, nonché specificare l'indirizzo di un eventuale host Dmz, nel caso le Nat Special Applications offerte dal dispositivo non risultassero sufficienti.

Andrea Pogliaghi



Il broadband router di Unex permette di condividere su una Lan una connessione Dsl

dispositivo è altamente configurabile da browser e permette all'utente di adattarne il funzionamento secondo le proprie esigenze: oltre alle comuni opzioni "di sistema", relative all'impostazione di password di accesso o alla modifica dell'indirizzo Ip, è possibile intervenire nei sottocampi di Wan, Nat, Firewall e Routing. Più in dettaglio, si può impostare un server Dhcp per l'assegnazione dinamica degli indirizzi Ip dei client connessi all'IS050S in modo automatico e semplificare la gestione della rete locale. Sul fronte del Nat (Network Address Translation), il dispositivo Unex offre funzioni di Virtual Server e forwarding delle porte, che rendono possibile a un

Unex NexIP IS050s



I giudizi di CHIP sono illustrati a pag. 240

- Altamente configurabile
- Installazione semplice
- Prezzo convincente

CHIP VI DICE CHE

Il prodotto di Unex consente di condividere una connessione a banda larga tra più pc e offre interessanti funzioni di sicurezza

Tipo: Dsl/Cable Gateway
Porte: 4 Ethernet Rj-45 (Lan), 1 Ethernet Rj-45 (Wan)
Dotazione: alimentatore, Cd-Rom con driver, manuale utente
Produttore: Unex, www.unex-tech.com
Distributore: Prodatec, tel. 02/9396431
Prezzo: euro 49,50

Modem • U.S. Robotics SureConnect Adsl USB9000

Velocità massima

Grazie alla connessione guidata il modem Adsl Usb di U.S. Robotics si configura in pochi minuti

■ Una caratteristica distintiva del modem SureConnect USB 9000 è la qualità del corredo di accessori. Oltre al cavo Usb per il collegamento al computer, il cavo telefonico, il Cd-Rom con i driver e il manuale su carta in italiano, U.S. Robotics fornisce un microfiltro tripolare Sip passante. L'etichetta identificativa sul fondo del modem e la procedura guidata per l'installazione dei driver confermano che il costruttore ha localizzato l'apparecchio esplicitamente per l'Italia. Il modem si alimenta dalla porta Usb del computer a cui è collegato, assorbendo 500 mA, ed è conforme alla versione 1.1 del protocollo per garantire la compatibilità con qualsiasi computer con Windows 98 SE o versioni successive. Il corpo del modem, più grande della media, ha tre spie frontali che indicano l'attività sulla porta Usb, la presenza di portante Adsl e quella della tensione di alimentazione.

La guida descrive dettagliatamente la procedura guidata di caricamento dei driver per Windows, che inizia presentando l'elenco dei principali provider italiani per i quali U.S. Robotics ha già predisposto i parametri di lavoro ottimali, e prosegue guidando passo dopo passo fino alla connessione finale. Un punto migliorabile è la sicurezza: la connessione Adsl generata dalla procedura guidata non viene automaticamente impostata come predefinita, né viene abilitata la funzione firewall di Windows XP

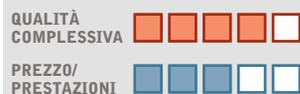


Un punto di forza del modem Adsl U.S. Robotics è la facilità di installazione

per proteggere il computer dagli attacchi degli hacker. Al contrario, la procedura guidata lascia attiva sulla connessione Adsl anche la funzione di condivisione di file e stampanti. Il funzionamento del modem è tuttavia affidabile e garantisce una connessione stabile e di qualità.

Paolo Canali

U.S. Robotics SureConnect Adsl USB9000



I giudizi di CHIP sono illustrati a pag. 240

- Funzionamento affidabile
- Buona documentazione
- Protezioni carenti contro l'intrusione

CHIP VI DICE CHE

L'installazione è più semplice rispetto a soluzioni concorrenti, ma chi vuole proteggersi deve rivedere le impostazioni di connessione

Tipo: modem Adsl esterno per porta Usb
Produttore: U.S. Robotics, www.usr-emea.com
Distributore: Actebis, Brevi, Computer Discount, Esprinet, Ingram Micro, Tech Data (vedi rubrica Aziende)
Prezzo: euro 119,00

In prova

Controllo remoto • Symantec pcAnywhere 11.0

Novità estetiche e funzionali

Symantec pcAnywhere 11.0 si rifà il look: interfaccia rivoluzionata che nasconde nuove funzionalità per la sicurezza dei dati

■ Il nuovo pcAnywhere 11.0 era atteso da tempo, dopo la release 10.5 del programma, distribuita anche per compensare l'incompatibilità della versione 10 con Windows XP.

Anche in questa versione restano due le principali operazioni consentite da questo applicativo: il controllo re-

documenti tra i due computer, di sincronizzare cartelle automatizzando le operazioni ripetute.

Su entrambi i pc il software deve essere presente: su quelli controllati, gli host, pcAnywhere rimane in attesa di una chiamata da parte del controllore remoto. L'host può

verificare che la nuova interfaccia rende più semplice l'accesso alle funzioni.

L'altra grossa novità riguarda gli strumenti: accanto al controllo remoto e al trasferimento file, infatti, pcAnywhere introduce una nuova funzione che consente di controllare rapidamente sia le

tenticazione: nel primo caso c'è la possibilità di inviare una serie di comandi all'host in modo che vengano eseguiti come una sorta di batch a uno o più pc.

Sicurezza garantita

Oltre alle autenticazioni standard, tra cui Ldap, Asd, Nds, Novell Bondery e quella nativa dei domini NT, spicca Rsa SecurID, verifica a doppia chiave (token e pin) che garantisce un ulteriore livello di sicurezza.

Per i pc dotati di sistema operativo Windows NT, 2000 o XP, infine, pcAnywhere introduce il tool Symantec Packager, che permette la creazione di versioni personalizzate del software, migliorando l'installazione in ambiente aziendale.

Gianmario Massari



La nuova interfaccia è una piacevole novità: a sinistra l'elenco delle funzionalità, a destra il desktop del pc controllato

moto e il trasferimento di file e cartelle.

Nel primo caso il controllore prende completamente il possesso del pc remoto, ne visualizza e controlla il desktop, può modificarne impostazioni e configurazioni, installare e usare software, gestire file e periferiche.

Il trasferimento file è l'attività meno evidente di pcAnywhere, così come di tutti i software di controllo remoto, ma non va sottovalutata: consente di scambiare

rimanere attivo fin dall'avvio del computer: pcAnywhere si può avviare come servizio del sistema operativo.

Una nuova interfaccia in stile Windows XP

La principale novità di questa versione è legata all'interfaccia: il restyling delle finestre è completo e colpisce ancor più perché un rinnovamento di questo livello non si avvertiva da molto tempo. A chi usa le vecchie release di pcAnywhere basterà però poco per

applicazioni e i processi attivi sull'host, sia di attivare un prompt MS-DOS, accedere alle configurazioni, ai registri di sistema, configurazione ed eventi, ai servizi e agli utenti collegati.

Modificato anche il trasferimento file: l'operazione avviene in background e non blocca la possibilità di effettuare altre attività sull'host.

Dal punto di vista delle funzionalità principali, le novità interessano la coda di comandi e i nuovi metodi di au-

Symantec pcAnywhere 11.0

QUALITÀ COMPLESSIVA

PREZZO/PRESTAZIONI

I giudizi di CHIP sono illustrati a pag. 240

- + Nuova interfaccia
- + Sicurezza SecurID
- + Nuova funzionalità di gestione remota
- Richiede IE 5.5

CHIP VI DICE CHE

La tanto attesa release 11.0 di pcAnywhere conferma le attese: è stabile, veloce e le modifiche funzionali e di interfaccia sono veramente ottime

Configurazione minima: Pentium, Windows 98 SE, 128 Mb di Ram, 35 Mb di spazio su hard disk, Internet Explorer 5.5

Produttore: Symantec, tel. 02/48270000, www.symantec.it

Distributore: rivenditori autorizzati

Prezzo: euro 299,00

In prova

Utility • **Steganos Hacker Tools 1.5**

Hacker veri o presunti?

100 tool di analisi, intrusione, sicurezza e violazione raccolti in un unico pacchetto

■ Si auto definisce “una temibile raccolta che comprende 100 dei programmi più pericolosi utilizzati dai pirati informatici”: si tratta di Steganos Hacker Tools, una collezione di sniffer, strumenti di attacco, mail bomber, nuker, password cracker.

La confezione, con il simbolo del Chemical Hazard ben visibile, accende l'interesse; pec-

oppure sono ormai inutilizzabili: a cosa serve Back Orifice, remote controller vecchio di almeno tre anni e ormai bloccabile da qualsiasi antivirus presente sul mercato?

Una delusione, insomma, per una raccolta di programmi che può essere considerata solo una panoramica di ciò che si può trovare in Rete e che può pertanto soddisfare appieno solo la curiosità del neofita che si avvicina per la prima volta al mondo underground del Web.

Di interessante c'è infine la classificazione dei software e la presenza, solo in versione dimostrativa, dei prodotti di sicurezza di Steganos.

Gianmario Massari



La classificazione e catalogazione di programmi e tool sono forse l'aspetto più interessante del prodotto

cato, però, che il prodotto non sia altro che una selezione poco ragionata dei software freeware e shareware per condurre generici attacchi in rete.

Nulla di nuovo, insomma: tutto materiale che si trova, più aggiornato, su qualsiasi sito hacker in giro per la Rete.

Nella confezione alcuni dei tool sono già superati (è il caso di GFI LANGuard, di cui è presente la release 2.0, mentre CHIP ha da tempo già recensito la release 3.0), mentre altri o sono specificatamente studiati per alcune versioni di Windows e non sono installabili su altre,

Steganos Hacker Tools 1.5

QUALITÀ COMPLESSIVA

PREZZO/PRESTAZIONI

I giudizi di CHIP sono illustrati a pag. 240

- + **Classificazione dei tool di attacco**
- **Versioni superate di alcuni programmi**
- **Prodotti inutilizzabili e non multiplatforma**

CHIP VI DICE CHE

Un bel nome, una confezione ben studiata ma “sotto il vestito niente” o poco...

Configurazione minima: Pentium, Windows 95, 16 Mb di Ram, 10 Mb su hard disk
Produttore: Steganos, www.steganos.com
Distributore: Koch Media, tel. 055/3247352, www.kochmedia.com
Prezzo: euro 29,99

Utility • **Spydex Email Spy Pro**



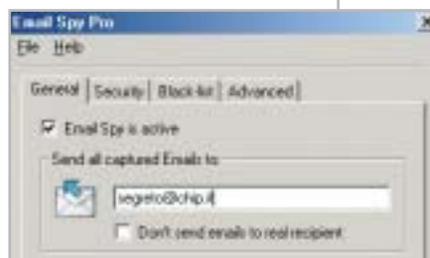
Grande fratello Smtip

Un programma per il controllo e l'inoltro della posta elettronica di un qualsiasi account...

■ Email Spy Pro è un sistema di monitoraggio e di filtro della posta in uscita dal pc su cui è installato questo piccolo programma. L'applicazione e la guida in linea sono in inglese ma le impostazioni richieste sono talmente ridotte al minimo da non ostacolare gli utenti che non abbiano dimestichezza con la lingua straniera.

Il pannello di controllo è costituito da una serie di schede che contengono le opzioni di configurazione del sistema di monitoraggio. La prima scheda richiede di indicare l'indirizzo e-Mail verso cui inviare tutta la posta in uscita dal pc; in questo modo è possibile controllare l'uso della posta senza accedere al programma di gestione dei messaggi ma semplicemente verificando il contenuto della casella indicata, possibilmente predisposta appositamente per svolgere la funzione di “spia” del traffico prodotto dal pc.

La prima scheda contiene anche l'opzione che permette di bloccare l'invio della posta al destinatario reale, realizzando così un filtro completo della posta in uscita. La seconda scheda imposta la password di accesso al programma (necessaria per evitare che altri utenti possano manometterne la configurazione) e permette di passare dalla modalità visibile a quella nascosta; è possibile infatti rimuovere dal pc ogni collegamento e traccia che possa rivelare la presenza del sistema spia, che rimane co-



L'indirizzo di destinazione della posta in uscita è l'unica informazione richiesta per avviare il sistema di controllo

munque attivo e può essere richiamato solo mediante una combinazione di tasti indicata dall'utente che utilizza Email Spy Pro. È possibile, inoltre, indicare un elenco di mittenti e di destinatari da escludere dal sistema di blocco.

Claudio Persuati

Spydex Email Spy Pro

QUALITÀ COMPLESSIVA

PREZZO/PRESTAZIONI

I giudizi di CHIP sono illustrati a pag. 240

- + **Controllo completo della posta in uscita**
- + **Possibilità di blocco della posta**
- + **Programma “invisibile”**
- **Comandi in inglese**

CHIP VI DICE CHE

Il sistema controlla la posta in uscita e copia i messaggi in modo assolutamente trasparente e non richiede alcun intervento sul server di posta

Configurazione minima: Pentium, Windows 95, 16 Mb di Ram, 1 Mb su hard disk
Produttore: Spydex
Distributore: Spydex, www.spydex.com
Prezzo: dollari 89,95

SOMMARIO

156	Mini-workshop Disabilitare il servizio news di Windows
158	Sistemi operativi alternativi Come bloccare lo spam in ambiente Linux
160	Indirizzi utili I siti dedicati al fenomeno spam
162	Il sistema SpamNet La collaborazione in Rete



Evitare la posta indesiderata

Basta spam!

Ogni giorno attraverso Internet arrivano innumerevoli messaggi pubblicitari e catene di S. Antonio. **CHIP** ha selezionato i migliori strumenti con cui bloccare lo spamming. *Di Markus Schmidt e Gianmario Massari*

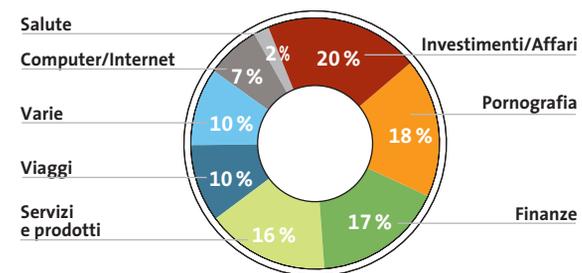
È una lotta accanita: ne vengono spediti ogni giorno tantissimi, si intrufolano attraverso la Rete, mettono alle corde i server di mezzo mondo e soffocano gli utenti privati con il loro numero. Sono i messaggi spazzatura: stiamo parlando di junk-mail, spamming, e-Mail promozionali e pubblicitarie mai richieste. Oggi però i messaggi di spam hanno vita dura: dei 6 miliardi di messaggi di questo tipo spediti ogni giorno "soltanto" 700

milioni raggiungono il loro obiettivo. Il resto viene catturato e bloccato. Si calcola, per esempio, che Microsoft Hotmail, da sola, respinga 2 miliardi di messaggi inutili ogni giorno. Mediamente, ogni giorno sopravvivono ai filtri e ai blocchi due messaggi di spamming per ogni utente Internet. Una media comunque troppa elevata: inoltre alcuni utenti non ricevono messaggi di questo genere, mentre per altri la quota di spam nei messaggi ricevuti può raggiungere il 90%.

Il lavoro degli spammer è uno solo: la caccia continua a nuovi indirizzi da colpire con la propria pubblicità. Contro l'invasione di spazzatura possono dare una mano vari programmi specifici, i cosiddetti antispam; anche le configurazioni di Outlook Express e quelle del sistema operativo possono rendere più duro il lavoro degli spammer. **CHIP** perciò presenta in questo articolo i migliori strumenti con i quali ci si può proteggere dalla fastidiosa pubblicità via posta elettronica e avere sul proprio pc una casella postale (quasi) esente da spam. Spieghiamo inoltre come evitare che il proprio indirizzo e-Mail possa cadere in mano degli spammer e riveliamo i trucchi con cui i provider riescono a bloccare lo spam.

CHI INVIA LA PUBBLICITÀ?

Chi spedisce messaggi pubblicitari via e-Mail sembra avere poca fantasia nei temi, ciò facilita il lavoro ai filtri antispam



Fonte: FTC

e-Mail spedite ogni giorno: **26** miliardi di cui messaggi di spam: **6** miliardi

dato mondiale; Fonte: IDC

Come bloccare gli spammer



Le più efficaci misure che si possono adottare per evitare che in poco tempo la vostra casella di posta si riempia di messaggi inutili e i trucchi per impedire che il vostro indirizzo venga scoperto

→ Pagine Web come fonti di indirizzi

Molti navigatori dispongono anche di un proprio sito Web personale. Queste pagine sono una delle migliori fonti per i collezionisti di indirizzi. Motivo: praticamente su ogni pagina Web è indicato un indirizzo per i contatti via e-Mail.

Problema: ovviamente i collezionisti di indirizzi sfruttano questa situazione. Proprio come i motori di ricerca scorrono attraverso le pagine Web alla ricerca di informazioni con i cosiddetti spider, chi fa spamming controlla i siti Internet alla ricerca di indirizzi di posta elettronica.

Soluzione: scrivete il vostro indirizzo e-Mail in modo che non possa subito venire riconosciuto da un programma di raccolta degli indirizzi. Si possono usare varie tecniche; a volte è sufficiente scrivere il proprio indirizzo usando una forma modificata, per esempio "administrator at sito punto it" invece del consueto *administrator@sito.it*. In questo modo si riesce a confondere alcuni degli strumenti di raccolta indirizzi degli spammer. I programmatori più esperti però riescono a superare questo tranello, adat-

tando i loro spider. La soluzione migliore è quella di inserire il proprio indirizzo e-Mail sotto forma di immagine. Aprire a tale scopo il programma di grafica preferito, scrivere l'indirizzo elettronico all'interno di un'immagine, magari modificandolo ulteriormente con lo strumento filigrana o con il deformatore. Il visitatore del vostro sito sarà sempre in grado di riconoscere il vostro indirizzo, ma gli spider andranno in tilt.

→ Giochi a premi come trappole

Che si tratti di vincere un paio di calze o 50 euro di Sms gratuiti, i giochi a premio si finanziano molto spesso tramite lo spamming.

Problema: perché sfogliare laboriosamente innumerevoli pagine Web quando si possono facilmente indurre i navigatori a fornire il proprio indirizzo e-Mail? Molti giochi a premio e inchieste tramite questionari su Web servono proprio a questo scopo.

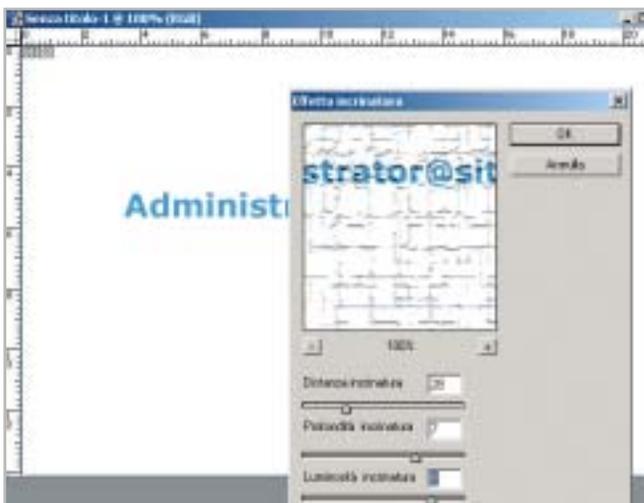
Soluzione: se si vuole proprio partecipare alla vincita di possibili premi, si deve assolutamente usare un secondo indirizzo di posta elettronica. Basta quindi creare un ac-

count secondario presso un qualsiasi fornitore di indirizzi e-Mail gratuiti, impostando il reindirizzamento automatico dei messaggi verso il proprio indirizzo primario. In questo modo se il secondo account viene sommerso da messaggi spam, basterà interrompere il reindirizzamento e il materiale indesiderato finirà nel nulla.

→ Verificare la posta sospetta

Alcuni spammer creano degli elenchi di indirizzi in modo del tutto casuale. Questa procedura richiede solo poco impegno e risulta assai economica.

Problema: se uno spammer vuole per esempio raggiungere con i suoi messaggi tutti i clienti di un provider Internet, per esempio internet-provider.it, cercando gli account con nomi utente di cinque caratteri, gli basterà creare un programma in grado di scrivere automaticamente a tutte le combinazioni di indirizzi e-Mail che vanno da *aaaaa@internet-provider.it* a *zzzzz@internet-provider.it*, salvando tutti i nomi in una rubrica di indirizzi. Naturalmente chi tenta un'operazione di questo tipo non sa quali indirizzi sono realmente esistenti: può però sfruttare due diversi trucchi. Il primo consiste nell'istruire il programma che invia le e-Mail a rimanere in ascolto delle risposte, scartando quelle per cui il server di posta di internet-provider.it segnala l'inesistenza dell'account. Il trucco



L'indirizzo e-Mail si può inserire sul proprio sito come immagine, più o meno manipolata: così si bloccano i motori di ricerca automatici



I messaggi Html rivelano agli spammer se un certo account è funzionante, dato che le immagini vengono caricate solo da un server

Strumenti antispam

è noto e molti server di posta evitano di rispondere quando sospettano di essere di fronte a un programma di questo tipo. Qui scatta allora il secondo trucco: capire quali sono gli indirizzi validi direttamente dagli utenti di internet-provider.it. Per indurre alla risposta gli utenti, la maggior parte dei messaggi spam includono un link che promette di eliminare l'utente dall'elenco dopo avere seguito un certo collegamento.

Soluzione: sembra quasi inutile dirlo. La risposta a un messaggio di questo tipo invece di interrompere lo spam lo avvierà. Non si deve quindi rispondere a questi messaggi, ma semplicemente cestinarli; altrimenti il mittente avrà la conferma che l'indirizzo di posta è valido.

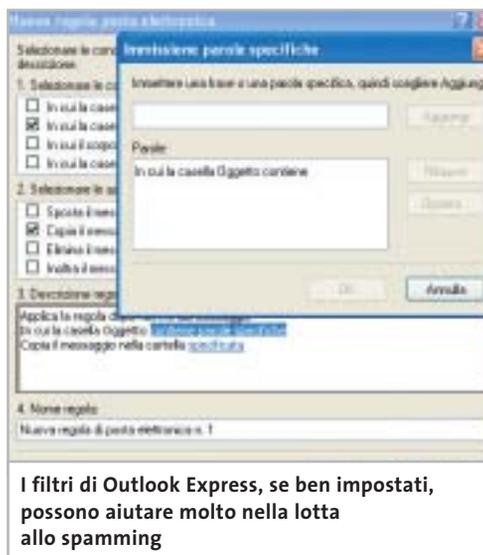
→ **Il trucco con i messaggi Html**

Si tratta di un trucco abile e fantasioso. Si parte dall'osservazione che i messaggi e-Mail sono più piacevoli se contengono delle immagini e delle formattazioni del testo e, molto più importante, possono scatenare azioni "lato server". Per queste due ragioni i messaggi Html sono i preferiti dagli spammer.

Problema: i messaggi e-Mail pubblicitari sono a loro agio con i messaggi in formato Html. Infatti il contenuto di questi messaggi viene scaricato da un server solo quando vengono aperti. Ciò significa che il mittente/spammer può monitorare il server Web su cui ha caricato le immagini e con un semplice script intercettare l'indirizzo e-Mail del destinatario del messaggio.

Soluzione: nel proprio client di posta elettronica si deve disabilitare la visualizzazione dei messaggi in Html, che conviene invece visualizzare in formato testo semplice. Per chi usa versioni poco recenti di Outlook questo suggerimento può provocare però dei problemi.

Infatti Microsoft nelle vecchie versioni dei propri client e-Mail non permetteva la disattivazione dei messaggi scritti in Html. In tal modo non solo gli spammer, ma anche i creatori di virus trovano una porta spalancata sul pc del destinatario sfruttando l'estetica di un messaggio. Solo a partire da Outlook 2002 Service Pack 1 i navigatori più attenti alla sicurezza possono porre rimedio alla situazione e visualizzare i



messaggi come semplici testi, privi quindi di rischi.

C'è però una speranza: nell'attuale versione beta 2 del nuovo Outlook 2003 i rischiosi messaggi Html vengono bloccati all'origine. Solo se lo si richiede esplicitamente i vivaci messaggi e-Mail vengono riattivati. Inoltre Microsoft ha integrato per la prima volta in Outlook 2003 un filtro antispam.

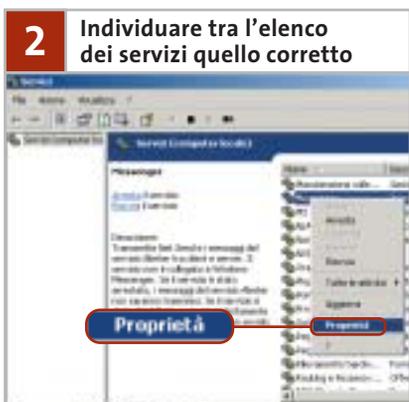
MINI-WORKSHOP

» **Disabilitare il servizio news di Windows**

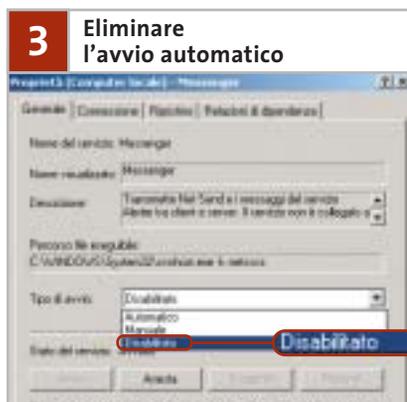
Il servizio di news integrato in Windows è perfetto per gli spammer: i messaggi pubblicitari compaiono direttamente sul desktop del navigatore. È un motivo sufficiente per disabilitare permanentemente la fonte dei guai.



1 Apertura degli Strumenti di amministrazione
Aprire il Pannello di controllo di Windows tramite Start/Pannello di controllo e commutare nella modalità di visualizzazione classica. Selezionare la voce Strumenti di amministrazione.



2 Individuare tra l'elenco dei servizi quello corretto
A questo punto fare un doppio clic sull'icona Servizi e nella finestra che appare selezionare la voce Messenger con un doppio clic. Si aprirà la finestra delle proprietà.



3 Eliminare l'avvio automatico
Nella finestra delle proprietà fare clic su Arresta, poi aprire il menu Tipo di avvio e selezionare Disabilitato. In tal modo si impedisce che Windows attivi il servizio al prossimo avvio del sistema.

Strumenti antispam

Mail gratuite senza spam



Chi naviga senza una tariffa flat è infastidito dal fatto che i numerosi messaggi spam rallentano il download. Un aiuto lo possono dare i filtri, che riescono a bloccare lo spamming prima che venga scaricato

Nella maggior parte dei casi, per chi utilizza caselle di posta gratuite, i messaggi vanno gestiti esclusivamente tramite il protocollo Pop3, che però presenta lo svantaggio di obbligare al download di tutti i messaggi di posta sul proprio pc, non essendo possibile eliminarli direttamente sul server del provider. In questo modo, purtroppo, si finisce per dover scaricare anche tutti i messaggi di spam. Si può tuttavia evitare questo inutile download se il provider è dotato di un filtro antispam.

Hotmail. Il servizio di posta elettronica di Microsoft ha da sempre attratto gli spammer, a causa dell'enorme numero di utilizzatori. A ogni account Passport di Microsoft, che è comunque necessario per il Messenger integrato in Windows, doveva evidentemente corrispondere una casella Hotmail.

Microsoft ha finito per reagire al rischio spamming: il produttore di software ha fatto recentemente causa a 15 mittenti di messaggi pubblicitari che avrebbero inviato agli utenti di Hotmail ben 2 miliardi di messaggi spam. Tuttavia Microsoft non ha ancora provveduto a munire Hotmail di un efficace filtro antispam per i propri account. Al momento

esiste una cartella Posta Indesiderata che, con diversi livelli di filtro (Standard, Aumentato ed Esclusivo) archivia lo spam: tuttavia con l'opzione Aumentato numerosi messaggi spam riescono a passare nella normale casella postale. L'opzione Esclusivo dovrebbe servire solo agli appassionati del Web, dato che passano il filtro solo i messaggi che provengono da mittenti appositamente classificati come desiderabili.

Tin.it. I servizi antivirus e antispam offerti da Tin.it sono compresi negli abbonamenti a pagamento offerti dall'Internet provider; i clienti del free Internet non dispongono dei servizi ma possono attivarli come opzione aggiuntiva, al costo di 2,95 euro/mese.

I messaggi di posta in ingresso contenenti allegati infetti vengono automaticamente eliminati, mentre la posta spam viene spostata in un'apposita casella accessibile via Web oppure utilizzando il protocollo Imap (opzione possibile solo per gli abbonamenti Internet/Adsl). La posta considerata spam non viene quindi cancellata ma parcheggiata temporaneamente in attesa che sia l'utente a scegliere di eliminarla. Via Web è possibile aggiungere nuovi filtri alle regole del mail

server di Tin: la versione Web della casella di posta di Tin permette di creare regole multicondizione tra loro.

Tiscali. La soluzione di Tiscali per proteggere la casella di posta dei propri abbonati si chiama SuperMail. Attivata gratuitamente per qualche mese, è ufficialmente diventato un servizio a pagamento con l'inizio dell'estate.

SuperMail si compone di un antivirus e di un tool antispam, oltre a una maggiore dimensione della casella di posta e del limite per l'invio e la ricezione delle e-Mail. Il prezzo di abbonamento è di 30 euro l'anno ed è interessante no-



Sulla sinistra, in rosso, l'accesso alla funzione antispam del servizio mail di Tiscali

tare come sia l'utente a poter definire la "cattiveria" dell'antispam agendo sulle opzioni da Web. Tre i livelli selezionabili: Basso, che contrassegna solamente le e-Mail considerate spam ma non le elimina dalla corrispondenza in arrivo; Medio, che prevede lo spostamento delle junk mail nella casella di spam (accessibile via Web o Imap, come per Tin.it); Alto, livello con il quale ogni messaggio sospettato di essere spazzatura viene automaticamente eliminato.

Yahoo!. Il servizio di controllo preventivo della posta di Yahoo! si chiama ANTI-spam. In questa cartella vengono trasferiti tutti i messaggi che il server mail di Yahoo! riconosce come spam. I messaggi possono essere visualizzati all'interno di un'apposita cartella. →

SISTEMI OPERATIVI ALTERNATIVI

» Come bloccare lo spam in ambiente Linux

I fan di Linux dotati di una casella e-Mail piena di messaggi pubblicitari possono passare al contrattacco con il programma Open Source Spam Assassin (www.spamassassin.org). La configurazione richiede la scrittura di un certo numero di file config e la gestione di procmail (www.procmail.org). Una volta effettuata la configurazione lo strumento assicura

che la posta in arrivo sia relativamente filtrata. A volte però l'impegno di Spam Assassin può risultare anche eccessivo, finendo per definire spam anche messaggi effettivamente utili. Perciò non si deve scegliere la cartella /dev/null come destinazione dei messaggi filtrati: altrimenti anche messaggi importanti verrebbero definitivamente eliminati.



I migliori programmi antispam



Quando i filtri dei provider non proteggono abbastanza, non resta che bloccare direttamente i messaggi. **CHIP** ha selezionato gli strumenti più innovativi ed efficaci che riconoscono lo spam prima che possa nuocere

Ella. Questo strumento (www.openfieldsoftware.com) si dimostra molto adatto per tutti gli utenti di Outlook che vogliono una gestione facile della protezione antispam. Il primo periodo di funzionamento del programma è di fatto di apprendimento, che serve per identificare i messaggi che l'utente considera spam e quelli considerati sicuri.

SpamKiller. Lo strumento di McAfee si rivolge ai tradizionalisti. Attualmente è disponibile solo in inglese. I difetti del prodotto sono i pregi dei concorrenti: non c'è la fase di auto-training di Ella, non ci sono elenchi di spammer come in SpamPal e non si applica il principio di comunità di SpamNet.

SpamKiller richiede regole di filtraggio che in base a determinati Oggetti identificano i messaggi come spam.

Il vantaggio del programma: interroga la centrale antispam di Hotmail, una funzione che finora possedeva solo Outlook Express (senza protezione antispam efficace).

SpamNet. Il principio del peer to peer non è valido solo per lo scambio di brani musicali via Internet: la società Cloudmark lo sfrutta per mantenere liberi dai messaggi spam le caselle postali degli utenti. Il concetto base è che quando un gran numero di navigatori collabora e riesce a creare un vasto database di spammer si possono poi filtrare efficacemente i messaggi spazzatura. Più di mezzo milione di utenti segnalano alla società ogni messaggio spam ricevuto. In tal modo Cloudmark può creare un elenco di mittenti di spam sempre aggiornato grazie al quale filtrare efficacemente la posta in arrivo ai propri utenti. Il tutto grazie a un piccolo plug in per Outlook, scaricabile dal sito di Cloudmark (www.spamnet.com). SpamNet funziona in modo egregio e sposta automaticamente i messaggi spam riconosciuti in una speciale cartella. Se comunque un messaggio riuscisse a passare, si può tramite un pulsante in Outlook inserire il messaggio nell'elenco "dei cattivi" di Cloudmark. Nelle nostre prove tuttavia SpamNet a volte si è dimostrato superattivo, segnalando come indesiderati anche messaggi perfettamente legittimi.

Solo le versioni beta di SpamNet sono utilizzabili gratuitamente: la versione finale richiede che si sottoscriva un abbonamento. Dopo 30 giorni di utilizzo di prova vengono richiesti circa 4 dollari al mese.

SpamPal. Il progetto Open Source di SpamPal (www.spampal.org) segue invece un concetto del tutto diverso. Questo intelligente strumento si installa sul pc come proxy locale: tutti i messaggi in arrivo vengono quindi per prima cosa esaminati da SpamPal, che poi li passa al client e-Mail. Questo apparente allungamento di percorso ha dei vantaggi: lo strumento può essere usato con diversi programmi di posta elettronica e come

INDIRIZZI UTILI

» I siti dedicati al fenomeno spam

Le risorse Web che parlano di spam, junk mail, protezione e violazione della netiquette sono tantissime. Tra le più interessanti vanno sicuramente suggerite quelle che si occupano degli abusi legati allo spamming, delle guide tecniche, delle esperienze di utenti comuni alle prese con i professionisti dello spamming.

www.nospamware.it/info/22: le ultime notizie e informazioni sullo spam.

<http://spamhaus.org>: il sito ufficiale di Spamhaus e della Spamhaus Block List (Sbl), sempre più considerato come il miglior modo di bloccare lo spam.

<http://spam.abuse.net>: la campagna contro gli abusi in Rete, purtroppo solo in inglese. Vi si possono trovare informazioni tecniche su software, suggerimenti per amministratori di sistema ma anche per utenti comuni e le frequently asked question sull'argomento.

www.internetprivacyfordummies.com: guida pratica alla privacy in Internet. Contiene un'enorme quantità di informazioni e molti suggerimenti antispam.

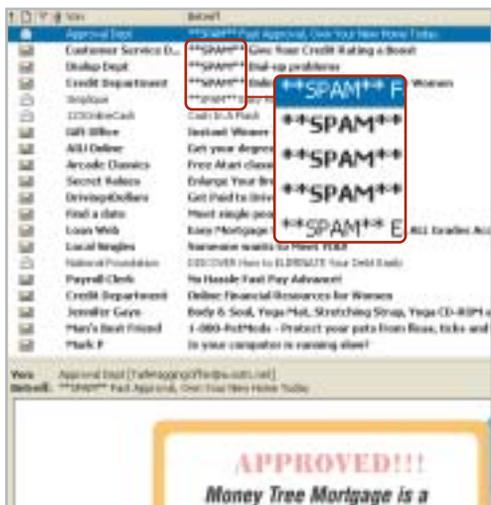
www.collinelli.net/antispam: vasto repository in lingua italiana che spiega che cosa bisogna fare per contrastare lo spam; dai filtri alle risposte alle junk mail, dalle segnalazioni ai provider alle più interessanti storie contro degli "spammatori professionisti".

www.nospamware.it: sito Web completamente in italiano con informazioni, notizie, segnalazioni, guide, tecniche e comportamenti legati al mondo della "posta spazzatura".

www.maxkava.com/spam/spam_intro.htm: il sito di Massimo Cavazzini, uno dei primi a citare in giudizio uno spammer accusandolo di fronte al Garante di violazione della privacy. Sul sito si può leggerne la storia, con estratti della sentenza del Garante (www.garanteprivacy.it). Un caso che andrebbe massicciamente ripetuto.

www.nic.it/NA/mailspam.html: come segnalare uno spammer alla Registration Authority italiana.

<http://listserv.nic.it/listserv/anti-spam.html>: la mailing list italiana sull'antispam gestita dal Nic (con la possibilità di abbonarsi).

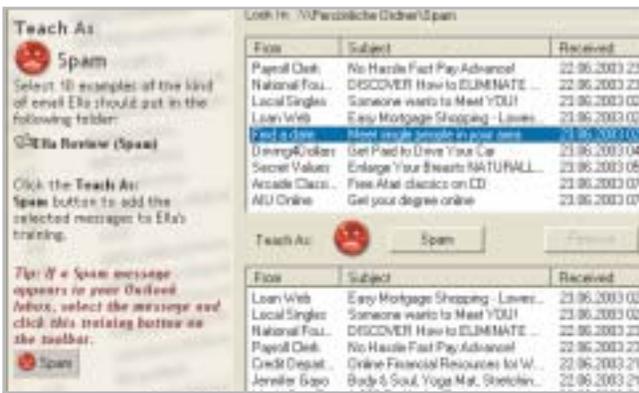


SpamPal identifica i messaggi spazzatura con l'etichetta **SPAM, che possono così essere eliminati usando le regole di Outlook

Strumenti antisпам



SpamKiller di McAfee filtra anche gli account Hotmail e blocca nei messaggi Html i contenuti attivi che spesso segnalano agli spammer se il proprio indirizzo e-Mail esiste



Il lungo periodo di training dello strumento antisпам Ella viene compensato dal funzionamento estremamente semplice nell'uso quotidiano

filtro in una piccola rete domestica. SpamPal completa la riga Oggetto di ogni messaggio riconosciuto come spam con

l'etichetta "***SPAM". Basta poi creare un'apposita regola nel client e-Mail affinché questi messaggi vengano spostati

in una cartella apposita. In Outlook Express i passi da eseguire sono quelli elencati qui di seguito:

- ▶ fare clic destro nella vista Cartelle su Posta in arrivo e selezionare Nuova cartella dal menù contestuale;
- ▶ dare alla cartella il nome Spam e confermare col clic su Ok;
- ▶ selezionare da menù Strumenti/Regole messaggi/Posta elettronica;
- ▶ nella nuova finestra premere il pulsante Nuova e selezionare l'opzione "in cui la casella Oggetto contiene parole specifiche" (sotto "Selezionare le condizioni della regola") e anche "Sposta il messaggio nella cartella specificata";
- ▶ nel campo Descrizione regola compare la nuova regola in chiaro. Fare clic su "contiene parole specifiche", marcate in colore blu, e sostituirle col testo **SPAM, fare clic su Aggiungi e poi su Ok;
- ▶ in modo analogo sostituire alla voce specificata, anch'essa marcata in blu, il nome della cartella Spam;
- ▶ dare due volte conferma su Ok. In questo modo in Outlook Express ogni messaggio che contiene **SPAM nell'Oggetto verrà spostato nella cartella degli scarti indicata.

IL SISTEMA SPAMNET

» La collaborazione in Rete

L'idea è piuttosto semplice: se a identificare gli spammer sono molti navigatori, tutti possono godere di una migliore protezione. Il plug in per Outlook di SpamNet invia l'impronta digitale (hash) di ogni messaggio al server centrale, che verifica se il messaggio è già stato riconosciuto come spam. Se il messaggio pubblicitario non era ancora noto basta un clic e il server lo includerà nell'elenco degli spammer.

