



Sono la vedova dell'ex-presidente dello Zaire, Mobutu Sese Seko: sembra incredibile che un messaggio della vedova di un importante uomo di stato africano (che non esiste più), morto cinque anni fa, arrivi nella nostra casella di posta elettronica. Eppure è così, e non solo: il messaggio è firmato dalla signora Miriam, che sta cercando un appoggio di natura bancaria, per recuperare alcuni milioni di dollari bloccati in una misteriosa banca svizzera. Come? Semplicemente aprendo un conto su un'altra banca e versandovi qualche migliaio di euro, come atto di buona fede. In cambio, Miriam farà transitare un fiume di denaro da quel conto lasciandoci una congrua provvigione.

È quasi inutile dire che siamo di fronte all'equivalente cyber di Totò che vende ai turisti la fontana di Trevi. Benvenuti nel mondo degli "scam", degli imbrogli in qualche modo legati a Internet. I messaggi che offrono di inondare il lettore con mucchi di improbabili ricchezze nascoste nel continente più povero della terra, in cambio del classico "piccolo anticipo" sono fastidiosi, ma sono solo un piccolo esempio dei tentativi di truffa che vengono perpetrati ogni giorno online, alcuni dei quali perfettamente riusciti. E se è facile cestinare le mail, altre forme d'imbroglio non implicano neppure una decisione cosciente da parte della vittima di turno.

La tecnologia, purtroppo, consente anche di mettere a punto imbrogli nascosti, come i tanto discussi dialer: programmi che molti ignari navigatori scaricano e installano sul loro pc per avere in "regalo" immagini più o

meno scollacciate, sfondi, suonerie per cellulari e altre amenità. Il dialer ha il brutto vizio (spesso mascherato in un "contratto d'uso" ambiguo e arzigogolato) di collegarsi a Pop, punti di presenza, corrispondenti a numeri telefonici a valore aggiunto. Tali numeri nella bolletta telefonica non vengono tariffati come gli altri, ma comportano l'esborso di parecchi euro al minuto. Il provider Tiscali ha fatto sensazione qualche mese fa, annunciando una rigorosa politica pubblicitaria che respinge le inserzioni Web dietro le quali si nascondono appunto questi veri e propri cavalli di Troia. Ogni volta che un banner rimanda più o meno direttamente a un file eseguibile (riconoscibile per l'estensione .Exe) è meglio drizzare le antenne. Prima di autorizzarne l'installazione, bisogna pensarci sei volte e leggere altrettante volte le condizioni d'uso che i fornitori del servizio "gratuito" sono sempre tenuti a esplicitare.

Detto questo, non bisogna certo eccedere in allarmismi di segno opposto. Navigare su Internet, partecipare alle aste, acquistare prodotti su siti di e-commerce non troppo credibili, interagire con la posta elettronica, comporta sempre alcuni rischi, che vanno dal semplice fastidio delle 20 finestre Web aperte a raffica o della catena di Sant'Antonio postale, fino ai danni materiali provocati dai virus o dagli imbrogli di natura finanziaria. Ma, al tempo stesso, bisogna ribadire che contro tutti questi rischi esistono valide barriere protettive, che molte volte richiedono una semplice dose aggiuntiva di buonsenso. In questa rassegna dedicata alla truffa, *CHIP* illustrerà i rischi correlati, le possibili difese e le contromisure. →



Truffe online

I soliti

Acquisti alle aste su Web, e-Mail che promettono guadagni miliardari, siti Internet che nascondono sgradevoli sorprese: i suggerimenti per riconoscere al volo i pericoli più diffusi online e difendersi adeguatamente. *Di Andrea Lawendel e Markus Schmidt*



TRUFFA 1

Aste online: chi offre di più? pag. 38
Come essere sicuri di ricevere la merce

TRUFFA 2

E-Mail: oltre lo spam pag. 42
Evitare le catene di sant'Antonio e i virus

TRUFFA 3

Software: dietro il banner pag. 46
Riconoscere dialer e spyware

TRUFFA 4

Siti Web: pagine con sorpresa pag. 48
Filtrare le finestre di pop-up

VENDESI

colosseo

Rivolgersi.....

Tel.....

ignoti



ASTE ONLINE: CHI OFFRE DI PIÙ?

Le principali aste online, come eBay, offrono alcuni utili strumenti per assicurare la soddisfazione del compratore e del venditore

L'esempio del sito internazionale di aste eBay è una delle poche grandi storie di successo della new economy, tanto più sorprendente se si pensa che quasi tutti gli imitatori di eBay sono falliti da tempo o sono stati rilevati dal colosso californiano. Sui siti nazionali e internazionali del-

la casa d'aste digitale si trovano sempre interessanti occasioni, senza contare il divertimento insito nel meccanismo dei rilanci. Alcuni browser contengono perfino funzionalità che aiutano a gestire la propria partecipazione alle gare, provvedendo a tenere sotto controllo in auto-

matico l'evoluzione dei prezzi. Ma i veri rischi sono sempre di natura economica e tangibile. Prodotti pagati in anticipo che non vengono consegnati, prodotti consegnati ma difettosi, prodotti venduti e spediti ma mai pagati, imbrogli assortiti. Ecco i principali ostacoli sul cammino della customer satisfaction, e come vanno aggirati.

Pagamenti anticipati

Il problema è vecchio come il mondo. La merce conquistata dopo un'accanita gara sul prezzo viene regolarmente pagata, con un qualsiasi strumento di pagamento, e il compratore si "dimentica" di spedirlo. Oppure, è il venditore in buona fede a spedire l'oggetto e a non vedersi mai accreditare il denaro.

La risoluzione non è immediata. Bisogna per prima cosa partire dal sistema di rating interno di eBay, che valuta il comportamento di venditori e compratori, provvedendo sempre a segnalare direttamente al sito le eventuali violazioni del regolamento.

Il consiglio per il venditore è sempre quello di utilizzare, se possibile, il sistema della consegna postale con pagamento contrassegno, che garantisce sempre l'esborso del denaro (il compratore, altrimenti, non riceve nulla). Ma se in linea di principio questo sistema sembrerebbe salvaguardare anche i diritti del compratore, ormai il metodo che si sta imponendo per garantire la piena soddisfazione di entrambi è il pagamento in Escrow!, cioè attraverso un fiduciario.

Da qualche tempo questa interessante formula viene messa a disposizione anche dai clienti italiani di eBay: si tratta del servizio di Deposito a garanzia, descritto all'indirizzo <http://pages.ebay.it/help/community/escrow.html>.

In sostanza, il servizio comporta il versamento del denaro concordato per una transazione su eBay presso un conto fiduciario di Escrow Europa (www.escrow-europa.com). Il compratore autorizza il trasferimento del denaro al venditore solo dopo aver ricevuto l'articolo acquistato e averne ispezionato il buon funzionamen-

(segue a pag. 40)

Il servizio di Deposito a garanzia fornito da Escrow! garantisce il pagamento e la ricezione dell'oggetto comprato all'asta su eBay

Per garantire ancora maggior sicurezza per le tue transazioni, alla conclusione della vendita eBay mette a disposizione il servizio di Deposito a garanzia fornito da Escrow! Da oggi puoi usufruire di tale garanzia e concludere gli affari senza preoccupazione, sapendo che i tuoi soldi e i tuoi oggetti sono garantiti sino al termine della transazione. Puoi comprare o vendere in tutto il mondo, scegliendo di effettuare acquisti o vendite con le principali valute, attraverso carte di credito, assegno o trasferimenti bancari senza nessun rischio.

eBay raccomanda l'utilizzo del servizio di Deposito a garanzia di Escrow Europa che riconosce come partner e consiglia di usare altri servizi Escrow che non siano citati in questa pagina.

Acquirenti **Venditori**

Compra **Vendi**

Quando fai un'offerta per un oggetto verifica prima se il venditore accetta di accettare il tuo denaro.

Quando metti in vendita un oggetto ricordati di scegliere "Accetto il servizio Escrow!"

FURTI DI PASSWORD

» Deviazione imprevista

La notizia è molto recente e riguarda proprio una frequentatrice americana di eBay, Deborah Fraser, che ha denunciato a CNet (www.news.com) un fatto molto increscioso. Tempo fa il numero di carta di credito della Fraser era stato trafugato. Il ladro di numeri si è servito di quella carta non per acquistare una pelliccia o un'automobile, ma per aprire un semplice dominio sul Web: *change-ebay.com*. Quel sito, si è scoperto successivamente, serviva per un altro tipo di furto, quello relativo ai nomi utente e alle password dei frequentatori del sito d'aste. Una volta in possesso di quel nominativo, in teoria è possibile accumulare un bel mucchio di soldi frodando gli altri compratori, prima di scappare con il malloppo.

Il meccanismo è semplice. Appoggiandosi sul sito change-ebay, il truffatore di turno spediva agli utenti di eBay fal-

si messaggi di allarme: "Caro amico, abbiamo motivo di ritenere che qualcuno abbia trafugato la tua password di eBay, per favore provvedi a cambiarla immediatamente". Spaventatissimi, molti utenti sprovveduti sono finiti direttamente su change-ebay.com, dove un computer registrava fedelmente ogni user id e password.

Non occorre dire che in casi del genere bisogna essere molto cauti. Il sito precisa ufficialmente di diffidare, segnalandole immediatamente ai servizi antifrode di eBay, le e-Mail che dovessero chiedere dettagli segreti come il nominativo utente o il numero di carta di credito (anche per questo motivo non vengono accettati user id equivalenti alla user id dell'indirizzo postale, quella che precede la @). Certe informazioni vanno protette con la massima attenzione.

ACQUISTI CON CARTA DI CREDITO

» **Per non dare i numeri**

La carta di credito è uno strumento che facilita gli acquisti, ma per moltissimi navigatori è quasi un tabù. Sui siti di e-commerce c'è chi si rifiuta categoricamente di fornire un dato evidentemente critico come il numero della propria carta.

La diffidenza è più che comprensibile ma, statistiche alla mano, emerge un dato che dovrebbe rassicurare. Le frodi via Internet rappresentano oggi una percentuale davvero trascurabile. MasterCard calcola circa 3.000.000 di transazioni online effettuate nel 2001 (il 75% su siti di e-commerce europei) dai circa 78.000.000 di carte in circolazione in Europa, per un volume pari al 2% del transato totale.

Una crescita del 100% rispetto al 2000. Tornando alle frodi, si calcola che nella nazione europea più matura sul fronte dell'utilizzo della carta di credito, il valore delle frodi ammonta ad appena 1.000.000 di euro al mese (70.000 euro in Italia). Nell'85% dei casi, il denaro "frodato" viene classificato tra gli episodi di rifiuto della transazione da parte del titolare della carta, che può essere insoddisfatto della merce acquistata, o essersi accorto dell'uso non autorizzato della carta da parte di un familiare.

In altri termini, è sicuramente molto più rischioso consegnare la carta al cameriere del ristorante che inserirla in un modulo elettronico Web, a patto che la pagina in questione sia protetta dallo "strato" di crittografia Ssl (Url preceduta da Https: e icona del lucchetto chiuso sul browser) e che il sito di e-commerce sia in qualche modo certificato.

Le soluzioni proposte dalle banche

Per risolvere definitivamente il problema della sicurezza degli acquisti online, l'e-Committee dell'Abi (Associazione Bancaria Italiana) ha messo a punto il sistema **Bankpass Web** (www.bankpass.it) e anche i principali circuiti di carte di credito hanno sviluppato tecnologie analoghe, come SecureCode di Mastercard e Verified by Visa, che verranno adottati a livello internazionale. Il funzionamento di Bankpass Web, che per la prima volta consente di utilizzare anche le carte Pago Bancomat per gli acquisti online, è tecnicamente molto semplice e non

comporterà l'uso di software particolari. Sarà tuttavia necessario attivare il servizio presso le banche che aderiscono all'iniziativa. Il sistema si basa, infatti, sull'uso di nominativi e codici personali che serviranno per autorizzare i pagamenti senza dover immettere il numero di carta di credito.

Una duplice sicurezza, per chi compera senza essere costretto a rivelare informazioni pericolose, e per chi vende perché il sistema è anche in grado di certificare la serietà del negoziante online e la solvibilità degli acquirenti. Un analogo sistema, "Paga con il Codice", viene adottato da

sono due varianti di carta Omnipay, Omnipay Prepagato vero e proprio e Omnipay Onphone, una card legata all'emissione di carte Visa BankAmericard che permettono di effettuare un acquisto online e autorizzarne il pagamento immettendo un codice Pin attraverso un Sms inviato con il proprio cellulare (analogo sistema adottato da Banca Sella con la carta ricaricabile Mobilmat).

Omnipay Prepagato funziona invece acquistando le normali carte prepagate che servono per le ricariche del cellulare. Sui siti convenzionati con il sistema, basterà immettere il codice a 14 cifre della



Su Commercio Elettronico.it si trova un'interessante panoramica relativa alle carte di credito prepagate

Banca Sella per i punti vendita federati al suo mall elettronico.

Un'altra soluzione per un acquisto online più sicuro è l'uso di una delle carte di pagamento prepagate oggi proposte da vari operatori. Purtroppo anche in questo campo si sono verificate truffe tanto più spiacevoli se si pensa che in teoria certi strumenti dovrebbero servire per combattere tali fenomeni. Il consiglio è di utilizzare solo gli strumenti proposti da istituti bancari attivi su scala nazionale o da operatori telefonici importanti.

Il bello delle prepagate

Non bisogna fidarsi di marchi del tutto nuovi e improvvisati. Sul sito di **Commercio Elettronico.it** (www.commercioelettronico.it/rubriche/prepagata.asp) vengono elencate le carte prepagate principali, a incominciare da **Omnipay** di Vodafone Omnitel (www.omnipay.190.it). Ci

carta e l'importo dell'acquisto verrà detratto dall'ammontare complessivo. Si tratta oltretutto di un ottimo sistema per i cosiddetti micropagamenti. L'utilizzo delle prepagate comporta ovviamente una piccola commissione in base a una scala di equivalente, che aggiunge ai prezzi degli articoli pagati una somma addizionale che verrà detratta dal valore attuale della carta.

Le altre carte prepagate descritte sono quasi tutte di origine bancaria e vanno richieste agli istituti emittenti (IntesaBci per Moneta Online, Banca Popolare Milano per Cartafacile Prepagata). Il costo di queste carte può richiedere un contributo di attivazione una tantum o un canone annuale, più eventuali commissioni fisse o a percentuale in base agli acquisti effettuati. In genere i costi annui sono paragonabili a quelli di una carta di credito convenzionale.



to o la corrispondenza alle sue aspettative o alle norme vigenti (eBay fa l'esempio di un software copiato o di una merce rubata). Se c'è qualcosa che non va, articolo e denaro ritornano ai rispettivi mittenti. Se tutto è regolare, il fiduciario provvede a versare il denaro al venditore e in cambio applica una commissione variabile tra il 2 e il 4% circa.

Se non si utilizza il sistema del Deposito a garanzia, chi compera e vende su eBay è comunque tutelato da un programma di protezione delle frodi che copre gli acquisti non andati in porto (per merce non spedita) fino a 230 euro, a patto che il valore dell'oggetto superi i 28 euro.

A questo proposito, si ricordi che i pagamenti con carta di credito sono comunque protetti dai vari circuiti di emissione, che consentono di stornare dal proprio rendiconto mensile gli importi relativi a prodotti acquistati fraudolentemente.

Prezzi fuori controllo

Molto spesso dietro l'eccitazione della gara si nasconde un fatto banale: niente garantisce che il prezzo pagato su eBay non sia del tutto fuori mercato.

Specialmente quando si tratta di acquistare articoli nuovi, magari nella categoria dell'elettronica di consumo o dell'informatica, i siti di e-commerce potrebbero offrire prezzi, servizi e soprattutto garanzie molto migliori.

Prima di cedere alla tentazione di quella che può benissimo essere una fal-

sa occasione, è opportuno uscire da eBay ed entrare in qualche Web shop. Vale la pena ricordare che esistono anche siti dove è possibile mettere a confronto immediato e automatico i prezzi rilevati su un congruo numero di importanti insegne dell'e-commerce nostrano: Buycentral.it, Costameno.it e Kelkoo.it.

Occhio al software

Acquistare i pacchetti software messi all'asta può essere rischioso anche quando il programma viene regolarmente inviato e funziona benissimo. Occorre sempre sincerarsi che il prodotto acquistato non

trovano informazioni e strumenti che aiutano a scoprire la natura illegale di un software. In caso di dubbio, bisogna rifiutarsi di installare un programma commerciale che sia stato consegnato su un Cd-R o in confezioni palesemente contraffatte o artigianali.

Giochi sporchi

Chiunque abbia partecipato a un'asta online conosce questo tipo di frustrazione. La nostra offerta è arrivata negli ultimi minuti, a volte negli ultimi secondi. Ma tanta pazienza è improvvisamente destinata ad andare delusa: a due secondi dal-

Item #	Brief Description of Item	High Bid	Bids	Qty	Profit	My Proxy	Time Remaining
205171439	M&T S&K Gold Watch - MUST SEE!	\$68.00	21	1	N/A	N/A	Auction Ended
205289994	Delightful Gallien Ship Brooch (\$4.25)	AU \$8.00	5	1	N/A	N/A	Auction Ended
1526874698	SPY FANTASY picture book SCHOLASTIC	\$6.00	6	1	N/A	N/A	Auction Ended
1816162157	Ford Ranger	\$3,700.00	24	1	N/A	\$11,050.00	1 hour, 59 mins +
62432356	SHINESTONE BRANCH BRIDCH	\$5.50	0	1	N/A	N/A	1 day 5 hrs
2013098126	Microsoft Office XP Pro Ver 2002 NIB - N/A	\$199.00	1	1	N/A	N/A	2 days, 0 hours +
1817227830	NEW Head i 510 Tennis Racquet	\$99.00	0	1	N/A	\$99.00	5 days, 23 hours +

Un software permette di battere tutti alle aste su eBay o Yahoo! Auction Sentry

sia una copia illegale, verificando che il Cd-Rom sia originale, che la confezione sia intatta (anche se consumata dall'uso), che i manuali e le cartoline con i numeri di licenza ci siano tutti.

Trovarsi in possesso di una copia pirata di un software equivale ormai a commettere un reato di ricettazione, e la legge non ammette l'ignoranza come giustificazione. Sul sito www.bsa.org/italia si

l'ora x, è arrivata un'ultima offerta da mezzo euro in più.

Purtroppo non c'è molto da fare. Alle aste via software partecipano anche... i software. Tra i molti siti Web e strumenti a supporto dei frequentatori di eBay ci sono anche i cosiddetti servizi "sniper", autentici cyber-franchi tiratori che partecipano alla gara per procura, utilizzando computer e linee di connettività a Internet molto più veloci del semplice modem, anche Adsl.

Uno dei più celebri tra questi siti si chiama Auctionsniper.com e offre servizi online, mentre Auction Sentry (www.auction-sentry.com) vende a 9,95 dollari un pacchetto da installare sul proprio computer. Vincere contro questi sistemi non è affatto facile quando si combatte con il dito - in carne e ossa - sul mouse o sulla tastiera. Per giocare ad armi pari bisognerebbe munirsi degli stessi strumenti, che eBay non ha la possibilità di vietare.

Al sito www.kelkoo.it è possibile confrontare i prezzi praticati dai principali negozi online per moltissimi prodotti



IL PARERE DELL'AVVOCATO

Dalla parte della legge

I consigli dell'avvocato per effettuare acquisti alle aste su Internet ed essere sempre soddisfatti

Apparse per la prima volta in Internet nella seconda metà degli anni Novanta, le aste online sono diventate subito una forte attrattiva per i frequentatori del Web, che in genere, però, per quanto attratti dai nuovi mercati virtuali, restavano e restano tuttora alquanto scettici sulla sicurezza e affidabilità di questa (come di molte altre) tipologia di attività svolta via Internet.

Ma vediamo, in maniera estremamente sommaria, come si relaziona con le aste il nostro legislatore. Abbiamo chiesto all'avvocato Gianluigi Ciacci di illustrarci le basi giuridiche delle aste online.

Acquisita la liceità delle aste online, come è tutelato il consumatore che usa questa modalità d'acquisto?

La stessa circolare sottolinea l'importanza della descrizione del bene: il venditore, o l'acquirente nel caso di asta inversa, Consumer to Business, deve fornire un'accurata descrizione del bene oggetto di vendita e, possibilmente corredarla di foto digitale, o addirittura di perizia, nel caso per esempio di mobili antichi. In caso di non coincidenza tra l'oggetto e la descrizione fornita sarà responsabile il banditore dell'asta se l'ha condotta, o il

Per quanto concerne poi le modalità di pagamento, come è meglio procedere?

La forma che sembra meglio tutelare l'acquirente, soprattutto nell'eventualità del pagamento anticipato all'invio della merce, è quella della carta di credito: molti enti gestori di carte di credito, infatti, danno una garanzia di rimborso all'acquirente nel caso di mancata consegna del bene. Ma, nel caso di asta tra consumatori, in cui il venditore difficilmente accetta tale forma di pagamento, il rischio della mancata spedizione rimane a totale carico dell'acquirente: questi, infatti, per una cifra normalmente esigua, spesso non intraprenderà le lunghe e onerose vie giudiziarie per il recupero della somma pagata, o per l'esecuzione del contratto.

Un altro aspetto importante riguarda la disciplina dell'errore: nel caso in cui l'acquirente sbaglia a digitare l'offerta, cosa deve fare?

Se l'offerta inviata fosse manifestamente superiore al valore del bene oggetto di asta, il contratto così concluso sarebbe annullabile per errore materiale riconoscibile dalla controparte, secondo le regole del codice che regolamentano il contratto in generale. Il rischio di un errore di tale tipo è di gran lunga ridotto nel caso di asta con riserva: qui chi partecipa fissa una cifra massima che è disposto a spendere, ma l'offerta di volta in volta considerata è solo quella sufficiente a superare le offerte degli altri possibili acquirenti, e mai quella massima indicata, che resta celata agli altri partecipanti.

Un consiglio conclusivo per chi vuole partecipare a un'asta online?

È fondamentale leggere attentamente le regole e i cosiddetti disclaimer fissati dai banditori, volti alla disciplina e regolamentazione dei rapporti nascenti dalle aste, auspicando presto un'autoregolamentazione di questo settore di mercato uniforme per tutti gli operatori.

<p>Descrizione</p> <p>Relogio- orologio alla svizzera a oro e acciaio prodotto in Svizzera limitata a 1000 esemplari ed autorivole in Italia, cassa in acciaio zaffiro del diametro di 43 mm, vetro zaffiro, cinturino a caviglia in acciaio POLYOT 2012, 1 anno di garanzia, autogaranzia, garanzia in più. L'orologio è nella foto accanto (escluso il 30 anni la vigilia è ereditabile nelle settimane a mezzo di un'azione OBOLINO INFOVO MAI DEDICATO).</p>	
<p>È molto importante che il venditore fornisca un'accurata descrizione del bene messo all'asta, corredandola di foto digitale</p>	
 <p>Offerta in base foto per trasparenza</p>	
<p>Contattaci per tutti i servizi da noi offerti da chi siamo.</p>	
<p>Dettagli per il pagamento</p> <p>Per ulteriori informazioni, vedi i termini di pagamento o la descrizione dell'oggetto oppure contatta il venditore.</p>	<p>Termini di pagamento</p> <p>Per ulteriori informazioni, vedi la descrizione dell'oggetto oppure contatta il venditore.</p>

Il giurista, in primo luogo, incontra una difficoltà nel considerare la liceità delle aste su Web. L'articolo 18 del D. Lgs. 114/98 vieta, infatti, le vendite all'asta realizzate per mezzo della televisione o di altri mezzi di comunicazione, tra cui senz'altro si deve comprendere Internet.

L'interpretazione di questa norma è stata data dal Ministero delle Attività Produttive nella circolare 17 Giugno 2002 n. 3547/C, che in parte ha anche individuato la disciplina applicabile a tale fattispecie.

Il divieto cade, in realtà, solo sulle aste svolte dagli operatori al dettaglio che acquistano beni per rivenderli al consumatore finale; ne restano quindi esclusi i grossisti o, comunque, chi non acquista professionalmente merci in nome proprio per rivenderle ad aree private.

Il venditore (l'acquirente nel caso dell'asta inversa) nel caso in cui il banditore abbia solo messo a disposizione il sito e la struttura: anche in tale ultimo caso, però, sarà di nuovo responsabile il banditore qualora non abbia esplicitamente posto a carico dei soggetti che conducono l'asta l'obbligo d'informazione e descrizione del prodotto.

Alle aste sono applicabili le normali garanzie riconosciute dal codice civile alle vendite in genere (garanzia per evizione, per vizi, per mancanza delle qualità promesse, oggi integrate dagli articoli 1519_bis e seguenti c.c.) con l'unica specificità che le garanzie dettate per l'acquirente sono normalmente escluse se il vizio era riconoscibile: qui, l'unica fonte per tale riconoscibilità è data proprio dalla descrizione fornita dal banditore/conducente.

L'AUTORE

Avvocato Gianluigi Ciacci, docente di Informatica presso la L.U.I.S.S. di Roma, titolare dello Studio Legale Ciacci, specializzato nelle problematiche del diritto dell'informatica e di Internet, direttore del sito giuridico Jci, Jus e internet. e-Mail avvocato@chip.it.



E-MAIL: OLTRE LO SPAM

Messaggi indesiderati, catene di Sant'Antonio e falsi annunci di virus: difendersi è possibile

Se si dovesse giudicare dal flusso di spam (i messaggi indesiderati e invadenti) provenienti dalla popolosa nazione africana, la prima conclusione da trarre è che la Nigeria sia un'autentica Svizzera equatoriale. Le risorse naturali, è vero, non mancano, ma qui si tratterebbe proprio di soldi sonanti, tutti misteriosamente nascosti dai numerosi dittatori africani, defunti o

solo quello che finisce nelle tasche del truffatore. Malgrado l'indubbio fascino esotico – e il divertimento nel leggerli – questi messaggi sono truffaldini, come mille altri che arrivano quotidianamente a milioni di indirizzi elettronici, dalle pubblicità su diete e pillole miracolose (come il campo di Pinocchio), alle profferte dei siti erotici, fino alle promesse di guadagni

te aziende italiane accusate, esplicitamente, di spamming. Si può leggere il testo ufficiale della decisione sul sito www.garanteprivacy.it. Molte informazioni di carattere legale si trovano anche su Diritto su Web (www.dirittoasuweb.com/approfondimenti/privacy.asp).

Come combattere lo spam? Innanzitutto rispettando una generale regola di prudenza e ripartendo le proprie attività su Internet avendo cura di utilizzare indirizzi diversi, ordinati per importanza e grado di riservatezza. Partecipare ai newsgroup con l'indirizzo usato sul lavoro, per esempio, è molto imprudente. È consigliabile piuttosto servirsi di indirizzi free, per esempio Hotmail di Microsoft. Il servizio, accusato in passato di essere un involontario motore di spamming, si è dotato infatti di potenti filtri antispam, che permettono di bloccare i messaggi in arrivo con diversi gradi di severità. Con le nuove opzioni di Hotmail è possibile impostare una lista di persone autorizzate a inviare la posta.

È opportuno anche iscriversi alle diverse newsletter utilizzando per ciascuna di esse un indirizzo speciale, possibilmente diverso da newsletter a newsletter. Certo, in questo modo aumentano le difficoltà di gestione degli account multipli, ma con programmi come Outlook questo aspetto è facilitato e questa prassi facilita enormemente la creazione di filtri personalizzati che ammettono solo il passaggio di messaggi provenienti da fonti sicure. Infine, una piccola regola che non costa niente è mascherare il proprio indirizzo all'interno dei client di posta, inse-

Un tipico messaggio che invita a partecipare a un sistema di multilevel marketing

Riccio per gioco
 Da: La Fortuna
 Data: martedì 26 novembre 2002 0.00
 A:
 Oggetto: Riccio per gioco

VORRESTI DAVVERO GUADAGNARE CON INTERNET ?

E bene, la prima cosa da fare è salvare su disco questa pagina per averla a portata di mano anche se il tuo PC non è connesso a Internet, poi copia tutto in Word o in Blocco Note e stampalo, così lo potrai leggere con più attenzione.

Questo Sistema è diverso da tutti gli altri, quindi se non ti fidi leggi con attenzione le istruzioni per valutarlo, e quando le avrai comprese ti assicuro che sarà per te IRRESISTIBILE la voglia di partecipare.

QUESTO E' SENZA DUBBIO IL GIORNO PIU' FORTUNATO DELLA TUA VITA !!
 IMMAGINA A COSA POTRESTI FARE CON 1.5 - 2 MILIARDI DI LIRE...

fuggiti chissà dove, e pronti per essere recuperati da vedove, figli, avvocati, gran ciambellani. Solo a patto, però, che i lettori dei messaggi e-Mail siano disposti ad anticipare qualcosa, aprire un conto bancario da qualche parte, far transitare su questi conti tesori in contanti e pietre preziose. Che ne direbbe di questi soldi il nigeriano medio?

Da almeno un paio di anni impervervano nelle caselle postali di mezzo mondo gli appelli che giungono da personaggi coinvolti in qualche modo con grosse somme di denaro nascoste in Nigeria. Chi prova a seguire il filo di questi appelli, si rende conto che questi tentativi di truffa sono attendibili e ben congegnati. Ma fin dai tempi dei quattro zecchini d'oro sepolti da Pinocchio nel campo dei Miracoli (il quinto zecchino era stato speso per rificillare lautamente il gatto e la volpe), anche i sassi sanno che il denaro facile è

miliardari in poche settimane, partecipando ai cosiddetti sistemi di multilevel marketing.

Il problema dello spam è del resto molto sentito a livello internazionale. In Italia l'estate scorsa è arrivata una clamorosa decisione dell'autorità garante della privacy, che ha bloccato i database utilizzati da set-

Diritto su Web propone numerosi approfondimenti sul tema della privacy e sul problema dello spamming

- Professione della Privacy e nella guida elettronica di Avv. Marco Barilli
- Privacy e Infortuni di Avv. Marco Barilli
- Privacy e informatica nella az. di Avv. Marco Barilli
- I contenuti del stampa via Internet con i casi di violazione della riservatezza nella privacy (D.L. 170/02) di Avv. Stefano Nasca
- Le norme di base dell'informatica - Informatica e privacy di Avv. Stefano Nasca
- Internet e privacy di Avv. Gian Paolo Saboni
- Videoregistrazione e Privacy: le nuove regole di Dink, Gianluigi Sisti
- Internet e Privacy (2ª parte) di Alessandro Sisti
- Le informazioni in tema di privacy e in tema della legge 173/2001 aspetti operativi di Avv. Stefano Nasca
- Le e-mail ed internet: qualche caso di violazione della privacy? di Avv. Stefano Nasca
- Pubblicità elettronica e privacy: un aspetto di violazione di posizioni? di Avv. Stefano Nasca

Truffe online

rendo nei campi Indirizzo per risposte: di Outlook o Eudora, un indirizzo modificato (per esempio: nomeNOSPAM.cognome@provider.it). Chi riceve il messaggio sa che per rispondere bisogna eliminare la stringa "NOSPAM", ma i programmi che cercano di individuare automaticamente gli indirizzi da riutilizzare per le campagne di spamming si troverebbero disorientati.

Catene da spezzare

Un altro grave problema dell'invasione postale riguarda messaggi che non sono per niente promozionali, ma che a volte possono addirittura sembrare umanitari. Tipico il caso degli appelli riguardanti bambini gravemente ammalati e bisognosi di cure costose. Invariabilmente il testo invita a rispedire una copia del messaggio a quanti più conoscenti possibile, sulla base di un presunto impegno, da parte dei

meno efficaci con le catene postali perché la maggior parte dei messaggi arrivano da persone che conosciamo e da indirizzi dai quali ci si aspetta messaggi interessanti, che non finirebbero mai in una black list.

L'unica arma di cui si finisce per disporre è lo scetticismo. Tutti i messaggi che invitano a ritrasmettere più copie della stessa mail ad altri indirizzi vanno tassativamente ignorati. Bisogna insomma spezzare tutte queste catene, anche quando si tratta di appelli e petizioni appa-

lito nel messaggio si fa riferimento a qualche innocuo file di sistema (famosissimo il caso di Sulfnbk.Exe, un piccolo eseguibile di Windows) che potrebbe essere infettato. Molti ci cascano, rimuovono il file e la cosa può anche finire lì, perché di solito il file in questione non svolge funzioni importanti. Ma quello che conta è il principio. Sull'allarmismo ingiustificato giocano anche molti banner pubblicitari che compaiono magicamente sullo schermo quando si visitano i siti Web.

La prima reazione di fronte a un messaggio relativo a un presunto virus è andare a consultare l'enciclopedia dei virus accessibile dall'Antivirus Center di Symantec, sviluppatrice del noto programma Norton AntiVirus.

La stessa società pubblica una dettagliata pagina sui falsi allarmi, che spesso risultano ancora più dannosi dei virus: www.symantec.com/avcenter/hoax.html. Molto famosa è la pagina sui "miti virtuali" (www.vmyths.com), piena di riferimenti ai falsi virus e ad altre forme di catene postali. L'autore, Rob Rosenberger, è convinto che dietro al fenomeno dei virus veri ci siano potenti interessi commerciali: una tesi piuttosto controversa.

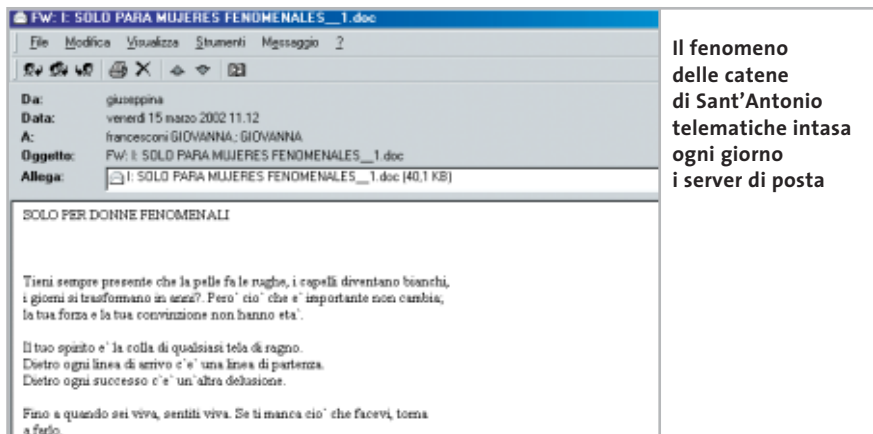
Da non dimenticare, poi, il sito <http://hoaxbusters.ciac.org>. Una pagina italiana sulla problematica antispam è di Leonardo Collinelli: www.collinelli.net/antispam.

Consigli utili

Dotarsi di un buon programma antivirus non basta per proteggersi del tutto dall'arrivo di contenuti indesiderati sul proprio computer. La posta elettronica è anche un potente veicolo di messaggi pubblicitari, catene postali, allarmi rela-



L'Antivirus Center di Symantec pubblica una dettagliata pagina sui falsi allarmi, che spesso risultano ancora più dannosi dei virus stessi



Il fenomeno delle catene di Sant'Antonio telematiche intasa ogni giorno i server di posta

provider, a versare una piccola somma per ciascun messaggio transitato in favore del piccolo paziente.

A volte si cercano semplicemente le cure di una malattia molto rara. In altri casi, meno strappacuore, le catene promettono semplicemente fortuna e felicità. In altri, viceversa, si cerca di diffondere un allarme ingiustificato su sostanze chimiche, farmaci, alimenti. Insomma, il fenomeno delle catene di Sant'Antonio, già piuttosto fastidioso con la posta cartacea, con Internet è diventata una vera peste. Con l'aggravante dell'incurabilità. I filtri e i sistemi antispam descritti finora sono molto

meritorie. Per essere davvero efficace, una petizione deve essere firmata da molte persone, ma deve allo stesso tempo pervenire ai veri destinatari, cosa semplicemente impossibile con una catena postale.

Sarà vero virus?

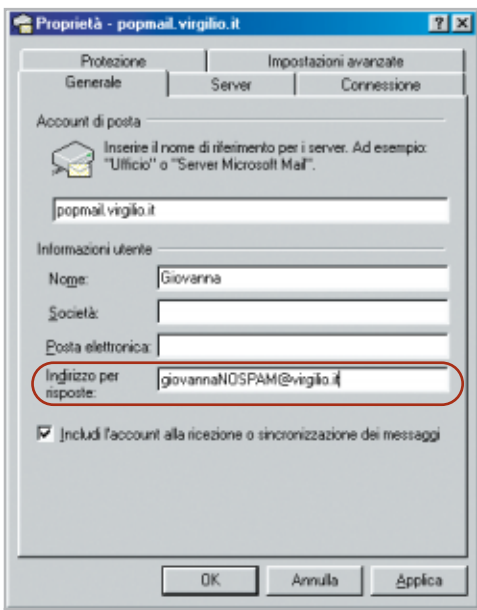
Una particolare variante delle catene di Sant'Antonio elettroniche è costituita dai messaggi che avvertono della possibile presenza di virus sul computer del destinatario. Nove volte su dieci si tratta di autentiche bufale (in inglese "hoax"). Di so-

Truffe online



tivi a virus del tutto inesistenti. Il buon-senso, l'intelligente impiego dei filtri di cui ogni client di posta dovrebbe essere dotato e il ricorso a software e servizi specifici può aiutare a ridurre al minimo questa grave forma di violazione della privacy online.

1. L'uso oculato degli indirizzi di posta di cui si dispone è la prima regola. Grazie alla possibilità di gestire più account con lo stesso programma (Outlook Express o Eudora), si possono organizzare diverse cartelle da assegnare ai messaggi personali o alle varie newsletter ricevute. Ogni indirizzo deve essere comunicato so-



Per difendersi dallo spamming è bene impostare nell'apposita finestra del client e-Mail un indirizzo per le risposte modificato

lo ai potenziali mittenti autorizzati. Un'altra buona regola è mascherare gli indirizzi inseriti nei campi Indirizzo per risposte: del client utilizzato per la posta con stringhe che modificano in chiave anti-spam il formato originale.

Per esempio nomeNOSPAM@pinco-pallo.com, o meglio ancora cose tipo "nome(dot)cognome(at)provider(dot)it". Di fronte a queste modifiche un lettore umano saprebbe come fare, mentre un software istruito per estrarre automaticamente gli indirizzi di e-Mail da pagine Web e newsgroup si troverebbe disorientato.

2. Outlook Express è dotato di potenti funzioni di filtraggio, le cosiddette regole (Strumenti/Regole Messaggi/Posta elettronica...). Impostando una nuova regola è possibile creare un meccanismo che cancella o rispedisce al mittente tutti i messaggi che non rispondano a determinate condizioni. La misura più drastica ed efficace è impostare una lista di mittenti autorizzati con la condizione In cui la casella Da contiene contatti.

Altre condizioni permettono di filtrare i messaggi per dimensione, tipo di soggetto, tipo o numero di allegati, livello di priorità. Analoghi strumenti sono a disposizione di chi utilizza la versione commerciale o quella finanziata da messaggi pubblicitari di Eudora (Tools/Filters/ New) e di altri client, come Pegasus Mail. Chi si serve di servizi di posta basata su Web, come Hotmail, può ricorrere a barriere del tutto simili, a partire dalle liste di mittenti autorizzati.

3. Esaurite le misure individuali, esistono prodotti e servizi capaci di assicurare un ulteriore livello di protezione contro lo spam. Col tempo sono emersi tre tipi di corazza: i pacchetti software che estendono le capacità di filtraggio dei più comuni client di posta; le liste di proscrizione pubbliche, in cui un sistema centralizzato comanda i meccanismi di filtraggio installato sul singolo computer; infine, i moderni sistemi di posta permission-based.

Un recente servizio messo a punto dalla startup MailFrontier (www.mailfrontier.com) si chiama Matador e viene proposto agli utenti di Microsoft Outlook in attesa di un'imminente versione per Outlook Express. Matador aggiunge a Outlook funzionalità di filtraggio aggiuntive e permette di impostare elenchi di mittenti autorizzati a spedire i messaggi (tutti gli altri vengono eliminati).

In più, il sistema tiene un'aggiornata lista di organizzazioni di spamming e blocca tutti i messaggi provenienti da queste fonti sospette.

Un servizio analogo, Spamslicer (www.spamslicer.com) si basa su Web e



Matador 1.0 di MailFrontier consente di filtrare i messaggi di spamming: il software è disponibile per Microsoft Outlook

può funzionare con la posta di qualsiasi provider e con qualsiasi client. Il sistema prevede l'uso di identificativi che mascherano gli indirizzi di posta originali (è possibile impostare più identificativi per indirizzo), ma ha un costo, anche se tutto sommato supportabile: gli abbonamenti più economici costano 35 dollari per una durata di tre anni.

Infine, un economico pacchetto individuale, da installare sul proprio computer (compatibile solo con Microsoft Outlook) consente di implementare un innovativo sistema antispam "permission based". ChoiceMail di DigiPortal (www.digiportal.com) costa 40 dollari e si comporta come un vero maggiordomo. I messaggi di posta passano solamente quando provengono da una lista di mittenti autorizzati.

Quando un mittente sconosciuto cerca di contattare l'indirizzo protetto, ChoiceMail provvede a inviargli un messaggio in cui il mittente viene invitato a dichiarare la propria identità e l'argomento trattato dal suo messaggio originale. Se il mittente è in realtà il software utilizzato da uno spammer, questa risposta non arriverà mai. Un mittente con intenzioni serie non deve far altro che presentarsi. ChoiceMail avvertirà il suo "padrone" che potrà decidere se autorizzare il contatto o meno. →



VENDESI
colosseo

SOFTWARE: DIETRO IL BANNER

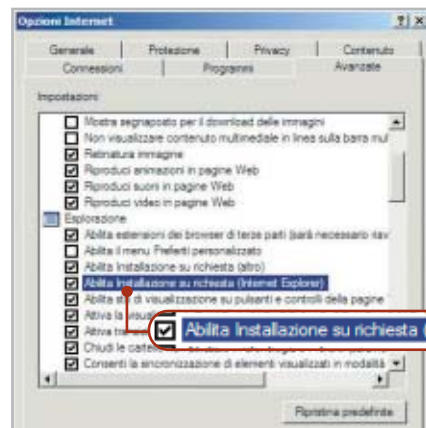
Come riconoscere dialer e spyware, per evitare bollette telefoniche astronomiche e violazioni della nostra privacy

Le denunce, sui molti siti Web dedicati alla tutela del consumatore online, si moltiplicano. Dietro molti banner che propagandano la possibilità di prelevare, magari "gratuitamente", immagini erotiche, suonerie per cellulari, sfondi, giochini vari e altre amenità, si nascondono degli autentici cavalli di Troia.

Il più delle volte, per aderire alle proposte e scaricare il materiale, il consumatore è tenuto a installare sul proprio computer un file eseguibile che stabilisce una connessione con un numero telefonico diverso da quello normalmente utilizzato per collegarsi al proprio provider. Il programma, chiamato dialer, si mette in contatto

favore l'offerta di servizi come l'accesso a Internet. Ma a volte chi offre questi dialer e i contenuti associati non gioca in modo del tutto pulito. Per legge sarebbe obbligatorio descrivere chiaramente le condizioni in base alle quali viene offerto il servizio, compresi i suoi costi dettagliati. Solo chi accetta in modo consapevole queste condizioni può accedere al servizio. Invece, molte volte il dialer viene installato in modo automatico, magari attraverso un semplice "Sì" su una finestra pop-up visualizzata da Windows.

Dopo poche settimane, l'importo accumulato in bolletta diventa pesante. In una clamorosa denuncia al quotidiano



La finestra di Internet Explorer 6 dove impostare l'autorizzazione all'installazione di un software, come un dialer

Windows chiede di autorizzare l'operazione.

Una misura più drastica, per chi utilizza un modem analogico, consiste nel chiedere al numero 187 di Telecom il blocco totale (e gratuito) di tutte le chiamate dal telefono di casa verso numeri 166, 709 e 899 (l'altra classe di numeri per servizi a valore aggiunto vocale).

Per informazioni su questa delicatissima questione ci si può rivolgere innanzitutto al sito del Ministero delle Comunicazioni, www.comunicazioni.it, sezione Risorse di numerazione. Siti come il già citato Punto Informatico o www.utenti.org danno molto spazio alla discussione in materia.



Il Ministero delle Comunicazioni fornisce indicazioni sui numeri a tariffazione maggiorata

Risorse allocate	
Ultimo aggiornamento: 23 novembre 2002	
Navvazioni	
Navvazione per servizi geografici 800	
Navvazione per servizi di tariffa preferita 144	
Navvazione per servizi di tariffa preferita 166	
Navvazione per servizi di addebito al chiamante (800 ex 187-8-8/567-8)	
Navvazione 800	
Navvazione 800 senza Regv	

con un numero molto "pesante" per la bolletta telefonica casalinga. Alcuni software sono programmati per effettuare una chiamata all'estero, altri utilizzano la numerazione audiotel contrassegnata dal 166, altri ancora la nuova classe di numeri per servizi dati a valore aggiunto 70x, dove x può essere il 2 oggi usato da molti provider dial-up, Tin compresa, o il 9. Si tratta di numeri gestiti da diversi operatori e tutti comportano il versamento di una tariffa speciale. Nel caso del 709, la connessione può comportare uno o più euro al minuto.

In apparenza, nessun problema. La numerazione 70x è stata istituita proprio per

online Punto Informatico (www.puntoinformatico.it), un lettore parla di 250 euro bruciati con qualche decina di tentativi di connessione (perché niente garantisce che il dialer funzioni a dovere, scaricando il materiale promesso). Come proteggersi?

Innanzitutto, utilizzando un browser aggiornato e sfruttando tutte le sue funzioni di sicurezza. Internet Explorer 6 ha, per esempio, un paio di voci in Strumenti/Opzioni Internet.../Avanzate, che recitano "Abilita Installazione su richiesta". Con questa opzione attivata, ogni volta che il dialer tenta di installarsi da solo,

La sicurezza dell'Adsl

Chi è stato imbrogliato da uno di questi servizi può cercare di risalire alle società o agli operatori che rendono possibili, spesso in modo del tutto legittimo e trasparente, questi servizi. Sul sito <http://digilander.libero.it/mamoFAQ>, alla sezione Diritti dei consumatori si trovano liste già pronte in formato testo.

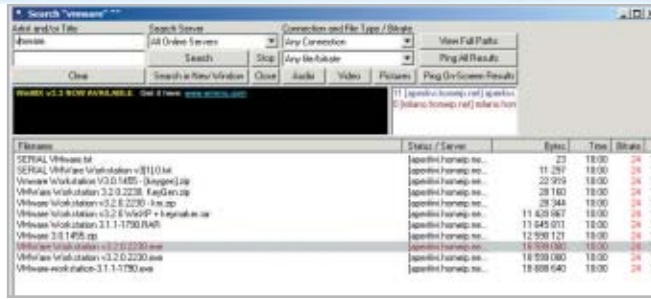
Un ultimo consiglio: in genere questi dialer sono "inermi" nei confronti di chi naviga su Internet attraverso una connessione Adsl, perché in questi casi il collegamento non passa da una sessione telefonica tradizionale. Sono stati, tuttavia, segnalati casi di dialer che disattivano la

Truffe online

connessione Adsl e cercano di attivarne una via modem. Il consiglio è di usare sempre la massima cautela e di leggere con attenzione tutte le note informative che i provider dei servizi 70x sono tenuti per legge a fornire.

Cavalli mascherati e spioni vari

I dialer mirano direttamente al portafoglio, ma altre tipologie di software aggressivi, magari con obiettivi meno dichiarati, rischiano di togliere tutto il buon umore alla vita dell'internauta. Questi ulteriori nemici rientrano nella generale categoria dei cavalli di Troia. Il navigatore che si preoccupa della propria privacy trova particolarmente fastidiosi i cosiddetti spyware, programmi che si nascondono nelle pieghe del sistema operativo e sfruttano le linee di Internet per trasmettere da qualche parte informazioni relative all'identità di chi utilizza il computer e al suo comportamento in Rete (siti Web visitati, indirizzi di posta usati e così via). Molti ritengono che anche l'adware debba essere bollato come



I programmi eseguibili prelevati da reti di scambio peer-to-peer possono nascondere spiacevoli sorprese

“spione”. Con il termine adware s'intende generalmente quella classe di programmi che cerca di finanziarsi attraverso la pubblicità. Uno dei più famosi è proprio il client di posta Eudora, disponibile anche in una versione completamente gratuita in cui vengono però visualizzati piccoli banner promozionali.

I vendor più seri cercano di proporre il modello adware in modo del tutto trasparente, dichiarando di aderire a rigorose politiche di salvaguardia della privacy individuale. La tesi è che l'eventuale spyware serva solo a monitorare gli interessi manifestati dal navigatore per poterli trasmettere banner sempre più in sintonia con le tematiche preferite. È consigliabile informarsi a fondo sulla questione, cercando il riferimento a queste

politiche sul sito Web di chi offre programmi gratuiti finanziati con i banner. Una seconda fonte di preoccupazione riguarda i file prelevati dai numerosi siti di programmi craccati, altrimenti conosciuti come warez, o scaricati sul computer attraverso una delle numerose reti di scambio basati su tecnologie peer-to-peer, come WinMX. Finché si scambiano file musicali, il rischio rimane confinato ai problemi di violazione del copyright, un problema comunque molto serio.

Problemi anche peggiori possono insorgere quando sul computer vengono scaricati file eseguibili, incluse le copie di programmi “ufficiali”, che non fanno assolutamente il mestiere dichiarato. O magari lo fanno, ma sono stati modificati con qualche funzione maligna.

NAVIGARE SICURI

» Uno stop alle intrusioni

Protegersi da spyware, cavalli di Troia e tentativi d'intrusione via Internet è possibile, ma comporta il ricorso a strumenti di firewall che non sono mai banali da utilizzare, e che possono interferire in modo pesante con le attività cui l'utilizzatore del computer è ben conscio (e lieto) di dedicarsi. Tutti i prodotti qui illustrati vanno dunque studiati attentamente, sapendo che in certi casi possono dar luogo a conflitti con programmi perfettamente leciti e non aggressivi.

Il problema dello spyware si affronta con due tool messi a disposizione da **Spychecker.com** e da Lavasoft. Il sito www.spychecker.com ha studiato un piccolo programma che, installato sulla scrivania di Windows, permette in qualsiasi momento di accedere al database di programmi adware/spyware gestito dalla stessa Spychecker. **Lavasoft** (www.lavasoft.de) è l'azienda che ha sviluppato il famoso programma Ad-aware, un firewall

che, oltre a proteggere dall'installazione di programmi nascosti, funge anche da tool di rimozione dei cavalli di Troia già presenti sul disco. È consigliabile utilizzare sempre una versione aggiornata, perché gli adware imparano presto a sfuggire al controllo di questi strumenti.

Programmi anti-intrusione ancora più estesi e potenti sono il gratuito **Zone Alarm** (www.zonelabs.com) o **Norton In-**

ternet Security, la suite commerciale di Symantec. Anche tra le reti di file sharing peer-to-peer cominciano a spuntare i primi segni di sensibilità al problema dei falsi. Su **eDonkey** (www.edonkey2000.com), per esempio, è stato istituito un servizio Donkey-Fakes che permette di individuare i falsi tramite un confronto online con un database di file messi in un'apposita lista nera (www.donkey-fakes.de.vu)



Ad-aware di Lavasoft protegge dall'installazione di spyware e rimuove quelli già presenti sul pc



SITI WEB: PAGINE CON SORPRESA

Alcuni semplici accorgimenti per navigare senza troppe finestre di pop-up e senza modifiche delle proprie impostazioni

Chiunque abbia navigato su Internet per più di due ore e su più di dieci siti, ha imparato a conoscere il fastidio delle finestre pop-up, che si aprono a ripetizione, e dei banner. I siti più violenti sono, tanto per cambiare, quelli a sfondo erotico o collegati ai casinò online.

Per scatenare la salva di finestre incontrollabili basta fare clic su una Url in apparenza del tutto innocente: quasi sempre, infatti, il navigatore è convinto di saltare verso un sito di suo interesse. L'effetto può essere molto spiacevole quando si sta navigando, perché la cascata di finestre copre tutto quello che si stava leggendo e l'unica forma di difesa consiste nel cercare di chiudere i disturbatori con

ripetuti comandi Alt + F4, o ricorrendo addirittura a Ctrl + Alt + Canc, un comando che però chiude tutte le istanze di Internet Explorer e costringe a rilanciare il browser. Il vaccino migliore contro questo tipo di malattia è il programma WebWasher, fornito gratuitamente per l'uso personale all'indirizzo www.webwasher.com. Il software permette anche di

applicare filtri contro la visualizzazione dei banner nelle pagine Web e altre forme di protezione. Tra le finestre che è possibile bloccare in questo modo, ci sono anche quelle che propagandano improbabili software di sicurezza o di "accelerazione" delle connessioni a Internet, un'altra sicura fonte di imbrogli.

Pagine iniziali dirottate

Un altro rischio molto spiacevole viene segnalato da molti utenti di Internet Explorer, che si ritrovano di colpo con le impostazioni della Pagina iniziale (quella che su cui si apre il browser una volta



Il software StartPage Guard evita che la propria homepage di Explorer venga cambiata automaticamente

PER LA PROMOZIONE

» Un motore davvero esoso

Recentemente è stata segnalata all'attenzione dei siti di tutela dei consumatori digitali, la vicenda legata a uno strano motore di ricerca, Europa Club, che sembra offrire un servizio gratuito riservato a coloro che vogliono promuovere le loro pagine personali (per la promozione di piccoli siti di commercio elettronico si paga una certa "fee"). Parecchi di coloro che hanno accettato il servizio inserendo l'Url personale, si sono visti recapitare la lettera di un legale di Bolzano, che pretendeva il pagamento di una somma arretrata.

In effetti, andando a leggere attentamente i termini di utilizzo (riportati solo in lingua inglese, nonostante la presenza di una homepage in italiano), si può leggere anche la regola che impone, per l'usufrutto gratuito del sistema, una sorta di scambio di Url.

In altre parole, se si vuole che Europa Club pubblichi l'indirizzo di una pagina personale, questa deve a sua volta contenere un link diretto a Europa Club. Se non viene inserito (come può accadere a

chiunque non legga attentamente le condizioni del contratto), il motore si riserva il diritto di chiedere del denaro, anche chiamando in causa uno studio di avvocati.

È ragionevole supporre che una clausola di questo tipo possa essere considerata vessatoria e quindi impugnabile, ma ciò non toglie che chi riceve l'ingiunzione deve affrontare parecchi fastidi. Europa Club, un servizio totalmente inutile visto che Google e gli altri motori ben più famosi hanno molte più probabilità di funzionare assai meglio come veicoli promozionali, va così ad aggiungersi alla marea di siti che offrono, magari a caro prezzo, prodotti "commerciali" a valore zero.

Attenzione in particolare a chi propone salatissimi programmi per la copia di Dvd e altre utilità di ripping attraverso il sito www.dvdsqueeze.com. Il rischio è di ricevere a casa – sempre che la consegna abbia effettivamente luogo – un Cd contenente una selezione di programmi shareware facilmente reperibili in Rete, senza sborsare nemmeno mezzo euro.

lanciato) modificate rispetto all'originale. Il problema si verifica con le versioni precedenti a Explorer 6, che in teoria dovrebbe avvertire l'utente quando è in corso un tentativo di modifica del valore inserito nel campo Pagina iniziale delle Preferenze.

Questo potrebbe essere il risultato di un'avventata installazione di un software clandestino, e purtroppo non c'è una soluzione immediata, perché se la nuova homepage non si può modificare attraverso il normale comando Strumenti/Opzioni Internet... di Explorer, significa che è stata apportata una modifica nel Registry di Windows e bisogna intervenire direttamente al suo interno.

Si può provare anche a riparare Explorer con l'installazione di applicazioni di Pannello controllo e l'opzione Correggi l'installazione di Internet Explorer visualizzata con il pulsante Aggiungi/Rimuovi... In futuro, si può evitare il problema con l'aiuto di una piccola utility chiamata StartPage Guard, che dovrebbe essere anche in grado di ripristinare i parametri truffaldinamente alterati. StartPage Guard è disponibile su <http://pjwalczak.com/spguard>. ■