

Problemi quotidiani nell'uso di Internet

ovvero come sopravvivere a spyware, dialer, virus, spamming ed e-mail
maliziose.

di **Alessio Sperlinga**
alessio@alessiosperlinga.it
<http://www.bambini.it>

Sommario

RINGRAZIAMENTI	3
PREFAZIONE	4
COSA CI IDENTIFICA QUANDO CI COLLEGHIAMO AD INTERNET.....	5
CHE USO PUÒ VENIRE FATTO DEI NOSTRI DATI.	6
SPYWARE	9
DIALER.....	11
TUTTE LE MALATTIE DELLA POSTA.....	14
VIRUS POSTALI ED HOAX	15
SPAMMING	17
CATENE DI SANT'ANTONIO ED E-MAIL MALIZIOSE.	18
CONCLUSIONI	19

Publicato la prima volta nel mese di maggio 2003
Do il consenso universale, mondiale, galattico al trattamento di questi dati ☺
solo per un uso NO-PROFIT e citando il nome dell'autore

Ringraziamenti

Grazie a :

Alberto Catagni per i consigli

Mio padre per i commenti

Pietro Calbi per l'attento lavoro di revisione. Il sito, da lui ideato e gestito, per dare

un giornalino scolastico all'Istituto presso il quale insegna è:

<http://www.itcmarchi.3000.it> .

Prefazione

Negli ultimi anni l'accesso ad Internet è diventato un servizio presente in qualsiasi personal computer, anzi spesso è una motivazione per acquistarlo.

Purtroppo di pari passo alla semplificazione nell'accesso ad Internet sono cresciute le insidie che si possono incontrare navigando.

Per questo motivo mi sono deciso a scrivere questa breve guida su come affrontare i problemi che mano a mano si incontrano nell'uso di Internet. Non è una guida per esperti e non ha alcuna pretesa tecnica. E' solo un testo divulgativo pensato per i principianti.

Questa guida è pensata per utenti che utilizzano personal computer con sistema operativo Microsoft Windows[®] dalla versione 95 in poi con il browser Microsoft Internet Explorer[®]. Chi usa sistemi operativi diversi, come ad esempio GNU/Linux o Unix è meno soggetto ai problemi che descriverò in seguito.

Per quanto riguarda la parte teorica fondamentale su cos'è Internet e come funziona, rimando al mio "Piccolo corso di Internet" scaricabile gratuitamente all'indirizzo <http://www.bambini.it/corso.html>.

Dedico questo testo a mio padre ed alle sue surreali telefonate di soccorso mentre naviga su Internet.

Buona lettura.

Alessio Sperlinga

Cosa ci identifica quando ci colleghiamo ad Internet.

Cominciamo con un esempio:

In un'azienda di solito ci sono più telefoni che linee telefoniche. Quando alziamo la cornetta il centralino ci dà la prima linea libera. Noi non sappiamo che numero stiamo usando, ma il centralino sì. La stessa cosa avviene su Internet. Quando ci colleghiamo il nostro fornitore d'accesso, detto ISP (Internet service provider), ci dà il primo indirizzo di rete libera, equivalente al numero di telefono della prima linea telefonica libera.

Come per il numero di telefono anche il nostro indirizzo di rete, detto indirizzo IP, è un'informazione conosciuta al nostro provider, ma anche a tutti i siti a cui ci colleghiamo. Le altre informazioni che i siti a cui ci colleghiamo possono raccogliere su di noi sono:

- Il nostro indirizzo di posta elettronica
- Il sistema operativo del nostro Personal computer
- Che programma stiamo usando per navigare
- L'indirizzo dell'ultimo sito visitato
- Il nome del server che ci permette di spedire la posta elettronica.

In pratica navigando su Internet seminiamo le nostre tracce dovunque.

Il nostro provider inoltre registra automaticamente il numero da cui chiamiamo, quello chiamato, la data ed ora di inizio e di fine collegamento e l'indirizzo di tutte le pagine che navighiamo.

E' come se ogni nostra telefonata fosse registrata.

Oltre a questo anche il nostro pc memorizza in apposite cartelle tutti i file che abbiamo visto navigando, perché per vederli devono essere inviati al nostro computer.

Se non li cancelliamo, chiunque utilizzi il nostro computer potrebbe essere in grado di vedere che siti abbiamo navigato. In Internet Explorer è possibile visualizzare la "Cronologia" attraverso l'apposito pulsante sulla barre degli strumenti o, dal menù Visualizza/Barra di Explorer/Cronologia. Ma attenzione, cancellare la cronologia non significa cancellare anche le pagine che abbiamo visitato.

Esistono i mezzi per proteggere la privacy, ma non esiste nulla di semplice. Ci sono programmi e servizi Internet che ci possono rendere anonimi nascondendo i nostri dati, ma rallentano la navigazione. Ci sono programmi, detti firewall, che ci proteggono in parte dai possibili tentativi di accesso al nostro personal computer e fra le varie cose ci rendono anche anonimi su Internet. Ma tutte queste cose richiedono conoscenze tecniche che l'utente medio non possiede.

Che uso può venire fatto dei nostri dati.

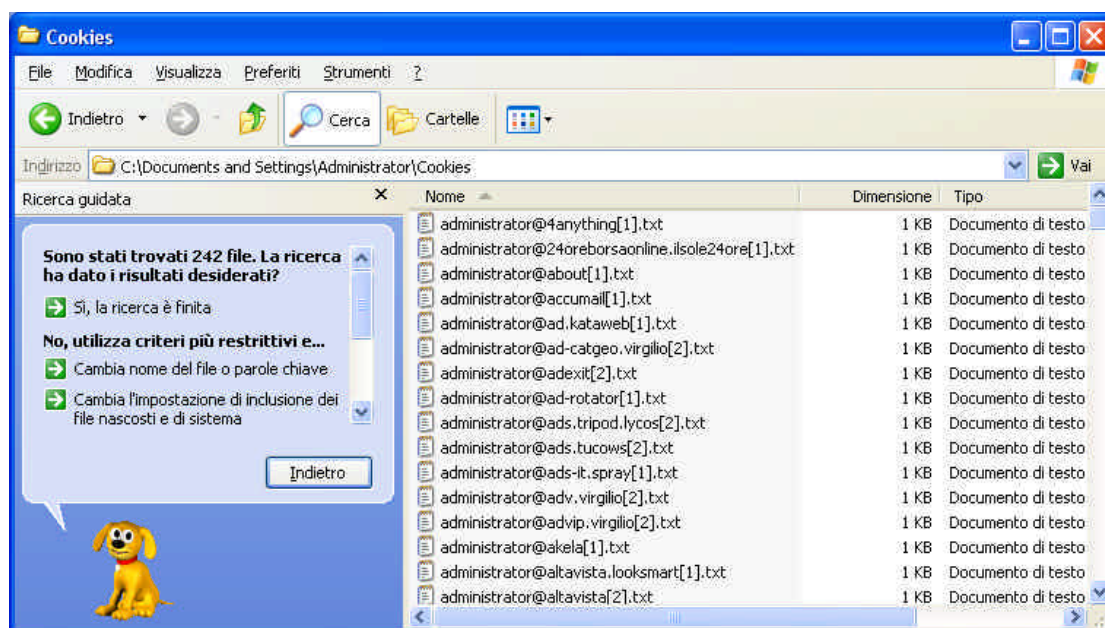
Dal punto di vista legislativo molti paesi difendono le informazioni personali con delle normative. Anche l'Italia ha la sua legge sulla Privacy. Ciò non toglie che tutti possono utilizzare i nostri dati a fini statistici, per esempio per sapere quante persone al giorno visitano il loro sito.

Un uso meno noto ma molto diffuso è la raccolta di informazioni statistiche su quanti vedono determinate pagine contenenti la pubblicità creata da società specializzate, dette società di advertising.

Vediamo in pratica cosa succede:

- Ci connettiamo ad un sito.
- Questo sito scrive un file di testo detto cookie (in italiano si traduce biscottino) sul nostro personal computer in una cartella apposita.
- Un cookie normalmente contiene un numero di utente che ci viene assegnato al volo, come se fosse un numero di codice fiscale, l'identificativo dell'azienda che lo scrive, la data è l'ora di creazione, la data è l'ora di scadenza. Nel caso ci siamo collegati ad un servizio personalizzato, come un sito dove giocare a scacchi, ci è richiesto un nome utente e password, che può essere memorizzato nel cookie per evitare di doverlo riscrivere ogni volta che ci colleghiamo a quel sito.
- Il sito a cui ci colleghiamo per giocare si farà una statistica delle nostre abitudini di giocatore cercando magari di farci qualche proposta commerciale, come partecipare a tornei a pagamento.

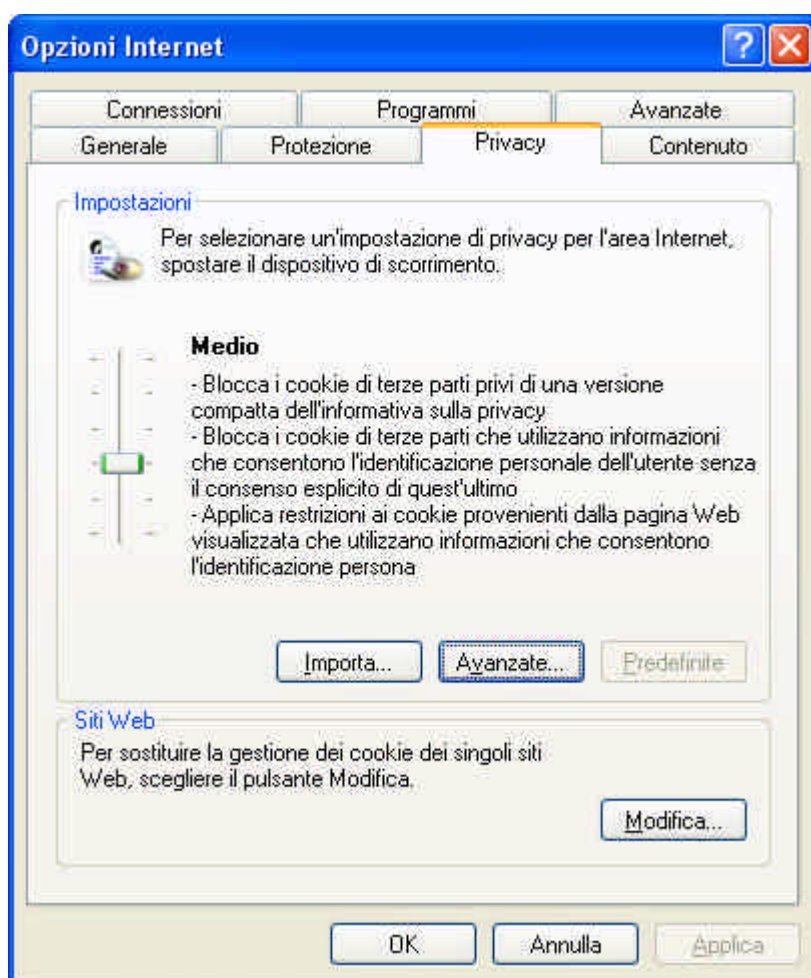
Ecco il risultato di una ricerca della parola cookie su un personal computer:



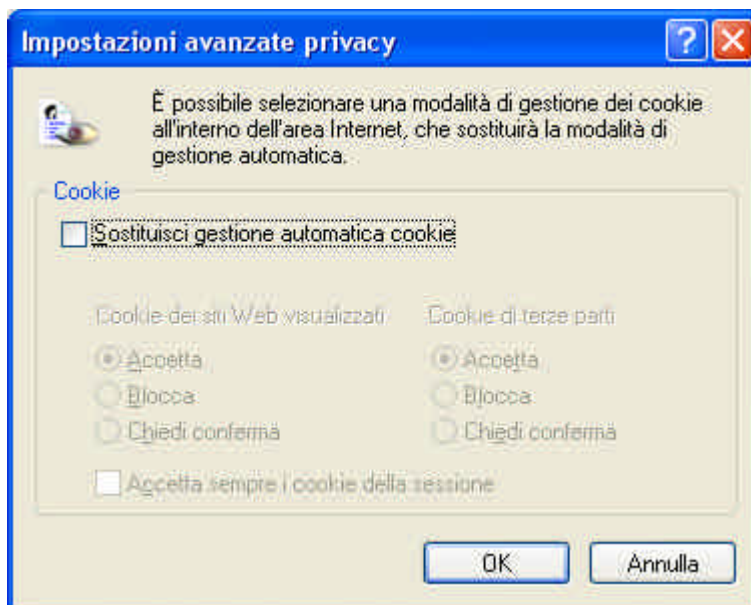
In tutta questa procedura non ci sarebbe niente di male se non fosse che a volte è usata in modo un po' diverso ovvero:

- Il cookie è creato da una società di advertising che lo legge quando ci colleghiamo ad un qualsiasi sito dove ci sono scritte pubblicitarie (dette banner) della stessa società. Una volta che ci ha riconosciuto memorizza su quali siti ci colleghiamo e quando.
- La società di advertising usa questi dati per dire ai suoi clienti quanta gente vede i suoi banner e per tracciare un profilo delle abitudini di navigazione degli utenti, ovvero per sapere quali siti abbiamo visitato, quante volte e per quanto tempo.

Sapendo quanto sopra possiamo decidere se accettare o no i cookies configurando il programma (browser) che usiamo per navigare. Nel browser Microsoft Internet Explorer c'è il menù Strumenti/Opzioni Internet e la voce Privacy come qui di seguito indicata:

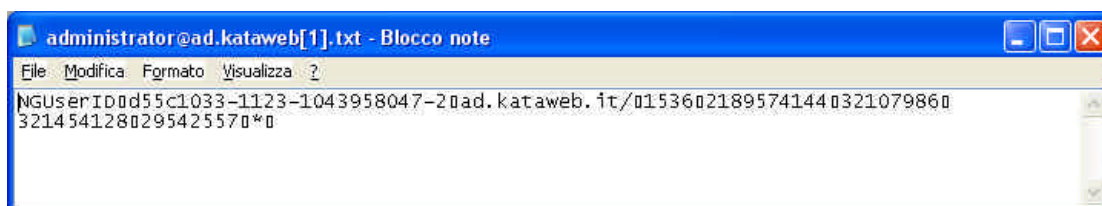


Di solito è anche possibile decidere di farci chiedere di volta in volta se accettare o no la scrittura di un cookie quando il sito a cui ci colleghiamo sta per farlo. Basta fare clic sul pulsante Avanzate del menù di cui sopra:



Oltre a questo è possibile dare il comando al browser per cancellare i cookie presenti su disco. In Explorer dal menù Strumenti/Opzioni Internet la voce Generale il pulsante Elimina Cookie.

Magari per curiosità guardate il contenuto di qualche cookie, troverete qualcosa di simile a questo:



Spyware

L'estrema applicazione di questi metodi si trova nei cosiddetti Spyware, ovvero software spia. Uno spyware è un programma che installiamo volontariamente nel nostro personal computer, di solito senza rendercene conto.

Una volta installato il programma aspetta che ci connettiamo ad Internet per inviare dati al suo "padrone" sui siti che navighiamo, o sui file musicali che ascoltiamo, o qualsiasi altra informazione sia programmato per raccogliere.

Ecco un esempio di cosa accade di solito:

- Andiamo da un amico e scopriamo che grazie ad un programma che ha scaricato da Internet fa una cosa che piacerebbe fare anche a noi, come ad esempio trovare e scaricare file da Internet con un programma ftp.
- Ci colleghiamo ad Internet e scarichiamo il programma, lo installiamo senza leggere il contratto che ci viene proposto a video ed iniziamo ad utilizzarlo.
- Durante l'installazione viene installato anche un programma spyware che entra in azione appena ci colleghiamo ad Internet.

Ancora più fastidiosi anche se meno maliziosi sono i programmi che ogni tanto caricano delle pagine pubblicitarie (advertising) in finestre che si aprono improvvisamente nel video senza alcun comando da parte nostra.

Rimuovere questi programmi non è semplice perché spesso sono nascosti e quindi bisogna identificarne i file. Spesso cancellando i file maliziosi il programma con il quale sono stati installati non funziona più. A volte lo spyware o il programma di advertising sono veri e propri programmi ma difficilmente hanno una procedura di disinstallazione. Inoltre se anche riusciamo a cancellarli spesso lasciano tracce di sé in altri file del sistema operativo, come nel file contenente i parametri di funzionamento di Windows, il registry.

Fortunatamente, come in ogni guerra fredda che si rispetti, ci sono dei programmi che ci aiutano in quest'opera di disinfestazione, i così detti programmi di anti-advertising e anti-spyware.

Ecco ad esempio la finestra di avvio di Lavasoft ad-aware:



I software "anti" di solito sono in grado di riconoscere molti spyware, i cookies delle società di advertising, le voci (dette chiavi) del registry di questi programmi e di rimuoverli su nostro consenso. Ovviamente ogni giorno i creatori degli spyware cambiano qualcosa per non farsi riconoscere e i creatori di programmi anti-spyware aggiornano le informazioni per rintracciarli.

Il tutto è diventato talmente normale che i programmi "anti" prevedono il comando per scaricare gli aggiornamenti delle informazioni per difendersi direttamente da Internet.

Attualmente i programmi "anti" più diffusi come Ad-aware sono gratuiti e facilmente rintracciabili su Internet. Basta ricordarsi di eseguirli una volta la settimana ed elimineremo la maggior parte di tutti questi software parassiti.

Un altro tipo di programmi utile per monitorare che programmi stanno cercando di accedere ad Internet dal nostro personal computer sono i cosiddetti Firewall, ovvero delle sorte di cani da guardia che servono per non far entrare o uscire nessuno senza aver chiesto il nostro parere.

I firewall per personal computer sono ormai abbastanza diffusi e ce ne sono di gratuiti come Zonealarm. Però non sono programmi in grado di decidere autonomamente cosa fare. Di solito le versioni per personal computer si limitano a darci dei messaggi in cui ci dicono che un certo programma sta cercando di accedere ad Internet, oppure da Internet sta cercando di accedere al nostro personal computer. Però sta a noi decidere se dire sì oppure no. L'utente medio semplicemente non è in grado di decidere. L'utente esperto nella stessa situazione si informa cercando su Internet il nome del file citato dal firewall per sapere che tipo di azione compie e poi decide se autorizzarne l'esecuzione.

Dialer

Il peggio che ci può capitare è di scaricare un dialer.

Il dialer è un programma che fa un numero di telefono. Purtroppo la telefonata costa vari euro al minuto. Inoltre il dialer spesso agisce senza che noi ce ne possiamo accorgere o lo fa in modo talmente strano che l'utente non capisce cosa sta succedendo.

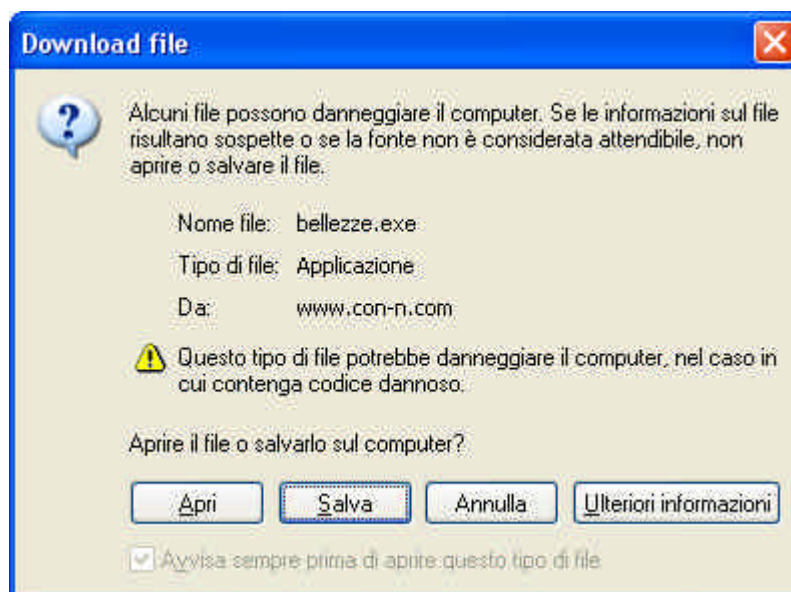
In pratica accade che:

- Ci colleghiamo ad Internet.
- Il programma dialer scollega la linea e fa il numero del servizio a pagamento.

Crediamo di essere connessi al nostro provider ma in realtà siamo connessi tramite una linea costosissima. Purtroppo la legge può fare ben poco perché per scaricare un dialer siamo noi a schiacciare il pulsante che ne autorizza l'installazione. Non è rara però anche la possibilità di inbattersi in siti che installano sul nostro computer dialer a nostra insaputa: se ci si accorge che ci stiamo scollegando e automaticamente ci si sta ricollegando... sarà meglio controllare la connessione!

Un esempio di come succede:

- Ci colleghiamo ad un sito dove vediamo un banner pubblicitario con scritte tipo "Suonerie per cellulari" o "I calendari delle modelle".
- Facciamo clic sul banner
- Ci troviamo in un sito con molte immagini e facendo clic su una qualsiasi diamo inizio alla scaricamento del dialer sul nostro personal computer.



Notate che il file Bellezze.exe termina con .exe. Significa che è un programma eseguibile immediatamente, spesso senza bisogno di alcuna operazione di installazione da parte nostra.

Più sottile può essere la richiesta di autorizzazione ad installare un oggetto software certificato in modo autonomo dall'autore del sito.
Appare una finestra come questa:



Un dialer funziona solo se abbiamo una linea telefonica normale (analogica) o isdn.

Se abbiamo un accesso ad Internet con linea Adsl o Hdsl in realtà non facciamo un numero di telefono e il filo del telefono collegato al modem viene usato come un cavo di rete collegato ad un concentratore (hub) del nostro provider. Quindi nessun programma può usarlo per fare telefonate.

Rimuovere un dialer è a volte difficile perché i programmatori che lo creano investono molto tempo a studiare come mimetizzarlo in mezzo ai file del nostro computer e farlo ricomparire ad ogni accensione, anche quando pensiamo di averlo cancellato. Un comportamento simile a quello di un virus.

L'unico modo per difendersi è prevenire. Dobbiamo stare molto attenti ogni volta che un programma ci chiede se vogliamo salvare un file sul nostro personal computer.

Nella peggiore delle ipotesi se abbiamo il sospetto che venga scaricato qualcosa sul nostro personal computer il consiglio è spegnere immediatamente il modem o il computer. Ci risparmieremo un sacco di fastidi.

L'unico aspetto positivo della paura generata dai dialer è che è un buon motivo per tenere d'occhio i figli che usano Internet e per investire in una linea Adsl.

Nel caso in cui il dialer si sia ormai installato sul nostro personal computer, l'unica soluzione è chiedere l'intervento di un tecnico sistemista per eliminarlo oppure installare un programmino come "STOP dialer" che non permette al vostro modem di chiamare altro che il vostro provider.

Potete anche chiamare il vostro provider telefonico per bloccare le chiamate internazionali con prefissi tipo 166, 899, 709 etc...
Purtroppo, anche se può apparire assurdo, alcuni operatori fanno pagare la disabilitazione dei numeri internazionali.

Tutte le malattie della posta.

Pensare a tutti i problemi legati all'uso della posta elettronica è come pensare alle intossicazioni alimentari. Le possiamo sempre prendere ma non possiamo fare a meno di mangiare, quindi ci fidiamo del supermarket.

Dico questo perché la posta elettronica è ormai uno strumento indispensabile. In molte aziende addirittura gli utenti sono autorizzati ad usare la posta elettronica mentre non hanno accesso alla navigazione su Internet.

All'inizio i programmi di posta elettronica potevano soltanto inviare e spedire files di testo. Poi è stato possibile allegare dei files ai messaggi. Poi qualcuno ha avuto l'idea di permettere ai programmi, ad esempio Microsoft Outlook[®], di poter eseguire altri programmi. Quello è stato il punto di svolta per la creazione di virus che usano i programmi di posta come mezzo di diffusione.

Come spiegato precedentemente il nostro indirizzo di posta elettronica si diffonde anche soltanto navigando su Internet. Oltre a ciò gli stessi provider, o i loro dipendenti infedeli, a volte hanno venduto gli elenchi di indirizzi di posta a società che diffondono pubblicità. Chi frequenta i gruppi di discussione, detti newsgroup, spesso si dimentica di mimetizzare il proprio indirizzo di posta e questo viene letto e archiviato dalle società pubblicitarie o specializzate nella raccolta di indirizzi e-mail.

Un altro problema, dovuto alla nostra natura sociale, è che tendiamo a leggere la posta che ci arriva e soprattutto a credere a quello che c'è scritto. Questo fa sì che e-mail scritte in modo convincente ci coinvolgano come in una catena di Sant'Antonio con risultati dannosi.

Questi concetti così diversi sono all'origine dei principali problemi di traffico di Internet, di intasamento delle nostre caselle di posta e della diffusione di virus informatici.

Nelle pagine seguenti è scritto come sono chiamati questi problemi, cosa sono e come affrontarli.

Virus postali ed Hoax

Grazie alla posta elettronica, o meglio grazie ai programmi che usiamo per spedire e ricevere la posta elettronica, detti client di posta, la diffusione di virus informatici è salita a livelli inimmaginabili prima dell'avvento di Internet.

Ci sono sostanzialmente tre metodi con cui si diffondono virus tramite la posta elettronica:

1. E-mail che contengono files allegati che sono virus o macro-virus, ovvero virus scritti nel linguaggio di programmazione eseguibile direttamente dal programma di posta o dal file allegato.
2. E-mail che utilizzano errori o falle nel codice con cui sono scritti i client di posta o la loro possibilità di eseguire altri programmi o macro-codice, ovvero codice scritto nel linguaggio di programmazione eseguibile direttamente dal programma di posta.
3. E-mail che contengono messaggi allarmanti, dette Hoax virus, ovvero delle bufale. Per esempio dei messaggi in cui c'è scritto che se trovate un certo file nel vostro personal computer va eliminato, oppure che se ricevete un messaggio di posta con un certo titolo non va aperto e quindi di avvisare tutti i vostri conoscenti del problema.

Per affrontare questo problema è necessario avere un comportamento sospettoso. Vediamo le caratteristiche di queste e-mail:

- Spesso gli indirizzi di chi ci scrive sono noti, ovvero sono clienti, fornitori o conoscenti a vario titolo. Per questo ci fidiamo e cominciamo a leggere la mail.
- Quindi la prima cosa da fare è non dare per scontato che una mail da un indirizzo noto è scritta volontariamente dal mittente. Spesso il mittente è rimasto vittima di un virus che usa il suo client di posta per spedire una mail contenente lo stesso virus alle persone inserite nella sua rubrica di posta.
- Anche se una mail arriva da un indirizzo noto, deve avere un contenuto corretto e coerente con frasi complete. Le mail infettate da virus ed inviate dai vostri conoscenti spesso contengono frasi sconnesse e senza senso prese a caso dal virus dalle mail già spedite dal vostro conoscente, e quasi sicuramente contengono un allegato. Non apritelo. Eliminate la mail e avvisate il vostro conoscente.
- Nel caso delle e-mail Hoax a volte sono così ben scritte che anche i tecnici sono tentati di diffonderle. Il loro unico scopo è terrorizzarci e spingerci a compiere un'azione, come inoltrare la stessa mail agli amici e quindi intasare ulteriormente il traffico su Internet, oppure cancellare un file su disco, provocando in realtà danni al funzionamento del sistema operativo. In questo caso è sufficiente non crederci o fare una ricerca su Internet per verificare se il virus citato esiste. Se scrivete hoax in un motore di ricerca scoprirete che tutte le società che creano programmi antivirus hanno molte pagine dedicate al fenomeno.

Cancellare le e-mail non è sufficiente.

E' necessario dotarsi di un buon antivirus e di aggiornarlo almeno due volte il mese.

Se ne trova ancora qualcuno gratuito su Internet, e comunque se comprate un computer normalmente lo trovate già installato. Per mantenerlo aggiornato basta collegarsi ad Internet, lanciare il programma dal menù Start/Programmi e trovare la voce di menù che parla di Update o aggiornamento. Purtroppo la tendenza attuale degli antivirus è di aggiornarsi per un anno e poi di richiedere un pagamento per poter proseguire gli aggiornamenti per un altro anno.

Anche i sistemi operativi vanno aggiornati, Nel caso di windows di solito è sufficiente connettersi ad Internet ed eseguire il menù Start/Windows Update oppure Start/Programmi/Windows Update. In questo modo manterremo aggiornati automaticamente anche il browser Internet Explorer ed il client di posta Outlook Express e quindi ci proteggeremo dai problemi esposti al punto due.

Spamming

Il nostro indirizzo di posta finirà rapidamente negli elenchi delle società che diffondono messaggi pubblicitari usando la posta elettronica.

Purtroppo fino ad oggi non sono stati trovati rimedi molto efficaci.

Quando troviamo la nostra casella di posta in arrivo invasa dalla pubblicità, si dice che siamo vittime dello spamming.

L'entità del problema è tale che si stima che circa un terzo delle email circolanti su Internet contengano spamming. Questo sta facendo sì che parecchi stati si stiano dotando di legislazioni contro le società che fanno spamming e ci sono già state numerose cause dove sono state condannate.

Ci sono varie strategie per difendersi da questo fenomeno:

- 1) Utilizzare uno di quei siti che ci danno un indirizzo di posta gratuito, come Hotmail o Yahoo, per crearci un indirizzo di posta da lasciare in tutti quei siti dove inseriamo i nostri dati per avere qualcosa in cambio, software o servizi gratuiti. In questo modo possiamo sempre andare a leggere la posta su Internet, ma sappiamo che non è niente di importante e possiamo sempre lasciare l'indirizzo inutilizzato e crearne un altro.
- 2) Chiedere al nostro provider di dotarsi di filtri anti-spamming o scaricare del software che ci dia questo servizio. Tenete conto che i filtri anti-spamming più efficaci al massimo eliminano il 40/50% delle mail pubblicitarie, ma a volte eliminano anche qualche e-mail che avremmo dovuto ricevere. In ogni caso se non abbiamo filtri antispamming ci conviene collegarci alla nostra casella di posta via web, ovvero da Internet, senza usare il client di posta, cancellare le mail pubblicitarie e poi scaricare la posta sul nostro personal computer.

In tutti i casi non facciamo altro che ritardare l'intasamento della casella postale che usiamo normalmente con amici e conoscenti. Ogni qualche anno saremo costretti a cambiare indirizzo e comunicarlo a tutti. Paradossalmente scopriremo che è molto facile aprire una nuova casella di posta che chiuderne una vecchia.

Catene di Sant'Antonio ed e-mail maliziose.

Le catene di Sant'Antonio si sono trasferite su Internet. In particolare le e-mail dove si annuncia che c'è un malato terminale che ha bisogno di soldi per curarsi o vuole che tutti gli scrivano una cartolina e che quindi noi diffondiamo ad amici, parenti e semplici conoscenti nella speranza di dargli una mano.

Ci sono stati casi eclatanti come quello di Craig Shergold di cui potete leggere scrivendone il nome in qualsiasi motore di ricerca.

Altro tipo di e-mail sono quelle con titoli come "Guadagna con Internet" oppure le strane e-mail che arrivano da un paese africano dove un signore ci chiede di dargli una mano a sbloccare dei fondi governativi inviando fatture o altre amenità che se ricevessimo con la posta normale straccерemmo al volo.

In questo caso è sufficiente cestinare. Non credeteci mai. Se volete potete sempre verificare facendo una ricerca su Internet e vedrete che al 99% sono tutte fandonie.

Però alcune vale la pena di conservarle, sono delle piccole opere d'arte.

Conclusioni

Per chi di noi usa Internet per lavoro o per passione da più anni, tutti i fenomeni descritti in questa guida sono fastidiosissimi.

Dico spesso ai miei allievi ed ai clienti che collegarsi oggi ad Internet è come se per andare al supermarket ci dovessimo mettere una tuta antiproiettile ed avere un'arma in tasca.

Basti pensare che la logica conclusione di quanto esposto in questa guida è che prima di collegarci ad Internet dovremmo installare sul nostro personal computer e mantenere aggiornati:

- Un programma antivirus
- Un firewall
- Un programma di anti-advertising

Oltre a questo dovremmo imparare a configurare il browser ed il programma di posta elettronica e ricordarci di effettuare l'aggiornamento del sistema operativo.

Personalmente ritengo che il rapporto fra il costo ed il beneficio nell'uso di Internet sia ancora a favore del beneficio.