E-SECURITY: LE E-MAIL E LA LORO SICUREZZA

v. 1.1

Questo tutorial è stato scritto da Gallerini Micaela (heba, heba.ry.mg@gmail.com), esso non vuole avere la presunzione di spiegare tutto fin nei minimi particolari, ma vuole essere un tramite tra gli utenti comuni e l'informatica, la sicurezza informatica, la programmazione. E' vero che esistono molti tutorial rivolti a questi argomenti, ma molti di loro sono esclusivamente scritti per utenti esperti o per esperti del settore. Ciò che mi sono riproposta è di scrivere una serie di tutorial che portino a capire l'informatica in modo semplice e poco contorto.

Indice

1. Le e-mail, i protocolli internet e gli RFC

L'e-mail è l'acronimo di *electronic mail* ha preso il posto della corrispondenza tradizionale, infatti mentre le poste ordinarie impiegano giorni per consegnare una lettera, l'e-mail arriva in pochi minuti o secondi.
Un'e-mail è di solito così composta:

mionome@nomedominio

dove *mionome* sarà il nome scelto o dall'amministratore della rete o dal richiedente dell'e-mail, potrebbe anche essere un nome di fantasia e *nomedominio* è il dominio di appartenenza che ogni e-mail deve possedere, per esempio se si avrà una casella di posta:

info@rosaventi.com

info è il nome scelto dall'amministratore e *rosaventi.com* il dominio di appartenenza, ed apparterrà quindi al sito (www.rosaventi.com); non è però detto che un dominio sia un sito privato come quello precedente, infatti ci sono numerosi hostes che permettono di avere un e-mail gratuita, *Yahoo* o *hotmail*, altri come *gmail* sono solo su invito di uno degli iscritti al servizio di mailing.
Le e-mail utilizzano un modo di ricezione ed invio di tipo *asincrono,* ossia non è necessario che entrambe le persone che inviano le e-mail siano collegati nello stesso momento. Esse utilizzano il protocollo internet[1] SMTP (acronimo di Simple Mail Tranfer Protocol), porta 25 per l'invio della posta, e protocollo IMAP, porta 143 o IMAPS [2] porta 993 per la ricezione della posta, oppure POP3 (Post Office Protocol) porta 110.
Vediamo esattamente come funziona:

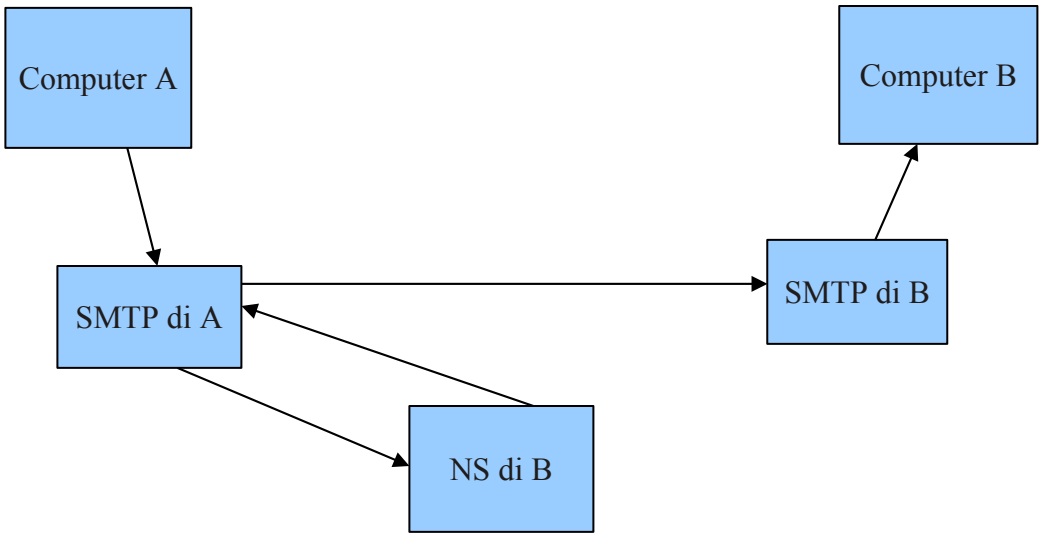


figura 1.

Nella figura1 è possibile notare che se invio un'e-mail dal *computer A* al *computer B*, il computer A la invia al mail server di A che richiede autorizzazione al Name Server di B (il dns locale) che controlla che l'indirizzo a cui si sta inviando l'e-mail esista realmente e sia configurato per poter ricevere le e-mail[3], ottenuta la risposta il mail server di A la invia al mail server di B tramite protollo SMTP, il

1 i vari protocolli internet sono regolati dai vari RFC, il protocollo SMTP dal RFC 821, IMAP e POP dal RFC 822 e la versione POP3 dal RFC 1939, Telnet dal RFC 854-855
2 IMAPS è il protocollo che utilizza gli ssl e la crittografia per la ricezione della posta
3 non è detto che tutti gli indirizzi di posta possano ricevere e-mail, di solito gli indirizzi non autorizzati a ricevere posta sono i risponditori automatici che vengono preimpostati per non ricevere e-mail di solito hanno anche nomi tipo

mail server di B processa l'e-mail e nel momento in cui il computer B la richiama tramite downloding della posta su un programma apposito (come può essere Outlook Express) il mail server la processa con protocollo IMAP, IMAPS o POP3 a seconda della tipologia di host utilizzato (es. Hotmail utilizza un protocollo IMAP, Yahoo un protocollo POP3).
Le e-mail ed il loro formato sono regolati dagli RFCs (Request For Comments), quelli sulla posta sono comunemente chiamati MIME, come comunque qualunque altro protocollo di internet.
L'**RFC 822** è il più vecchio e risale agli anni '70, il primo che ha dato un'indicazione su come dovevano essere scritte le e-mail, per esempio non devono essere utilizzati questi caratteri "<" o ">" per contenere il nome della persona quotata, ma possono essere utilizzati nel corpo dell'e-mail se questo comporta una difficile comprensione di chi quota e di chi viene quotato; attualmente è utilizzato questo carattere generalmente ">" per quotare un pezzo di e-mail. L'asterisco "*" è utilizzato per indicare la ripetizione di un elemento o parola. In esso sono anche contenuti i campi obbligatori o non obbligatori che un'e-mail deve avere per poter essere spedita, il campo "a:" oppure "da:", sono obbligatori mentre "cc:" o "bcc:" il corpo del messaggio o l'oggetto non sono obbligatori ma facoltativi.
L'**RFC 2045** stabilisce come il corpo dell'e-mail deve essere scritta, l'utilizzo di 7 bit od al massimo 8 bit per l'estensione del corpo della lettera, il testo deve essere testo "semplice" o "composito", quest'ultimo viene comunemente chiamato formato **html** che è quello che permette di poter inserire emoticons, sfondi colorati, piuttosto che colori diversi per le parole o permette di utilizzare il grassetto ed il corsivo per la scrittura, infatti anche l'utilizzo di html è conforme alle norme RFC, per quanto ne dicano alcuni.
Gli altri RFC che regolano la composizione e l'invio delle e-mail sono: **2046**, **2047**, **2049**, **2822**. In questi RFC vengono date delle indicazioni per poter scrivere un'e-mail correttamente, ma soprattutto le indicazioni vengono date agli hostes pubblici o privati perché si adeguino a tali norme, per cui nel momento in cui accediamo alle nostre caselle di posta, sia via web, sia tramite un programma di posta elettronica (Outlook piuttosto che Incredimail, Mozzilla Thunderbird, Kmail o Evolution) essi devono essere già adeguati agli RFC senza che chi utilizza questi servizi debba esserne informato.
Le e-mail sono anche regolate da una **netiquette**, RFC 1855, che indica come è meglio che vengano inviate le e-mail ed i vari testi che si postano su internet. Per fare alcuni esempi contenuti in questo RFC: è meglio ricordarsi che internet è un villaggio *multirazziale*, *multiculturale* e *multietico*, ognuno ha una sua etica personale e culture differenti anche all'interno dello stesso paese di provenienza, non tutti hanno le nostre stesse idee ed è quindi necessario avere un po' di buon senso e rispetto per tutti cercando di evitare i flame (denominazione non di insulto, ma di comportamento forte) e di rispondere con calma cercando non di imporre le proprie idee ma di apportarle al gruppo come conoscenza, ciò non va fatto però solo da una parte, ma **deve** essere fatto da tutte le parti che stanno corrispondendo tra di loro, se solo uno (o pochi rispetto alla totalità) continua ad utilizzare un linguaggio consono ed etico c'è il rischio prima o poi di sfociare in un flame megalomane corredato di insulti. Inoltre, viene indicato di scrivere i flame o comportamenti anomali con un on/off (es. Flame on, quando si comincia un flame, flame off, quando lo si finisce), oppure si può scrivere tra parentesi (es. l'indicazione di una frase detta ironicamente "frase ironica"), l'utilizzo delle emoticons che non hanno immagini o quelle con immagini per chi utilizza html (es. :P, che indica lo scherzo, o una battuta). Il quoting deve essere fatto solo per la parte che interessa realmente e non per tutta l'e-mail intera se non interessa, non è indicato in che punto bisogna scrivere il proprio pezzo se sopra o sotto, l'importante è capire cosa si sta dicendo e a quale pezzo ci si riferisca. Non solo questo RFC regola anche le mailing list e i loro moderatori.
Ricordarsi comunque che chiunque scrive non sempre conosce gli RFCs, i programmi sono fatti da esseri umani quindi non sono perfetti e possono sbagliare, se un programma sbaglia non è colpa di chi invia l'e-mail o il testo, ma è sicuramente un bug di programmazione, utilizzare il proprio cervello per capire le varie situazioni è sempre meglio, avere un minimo di buon senso e di comprensione e rispetto per gli altri, anche.

---

noreply@nomedominio

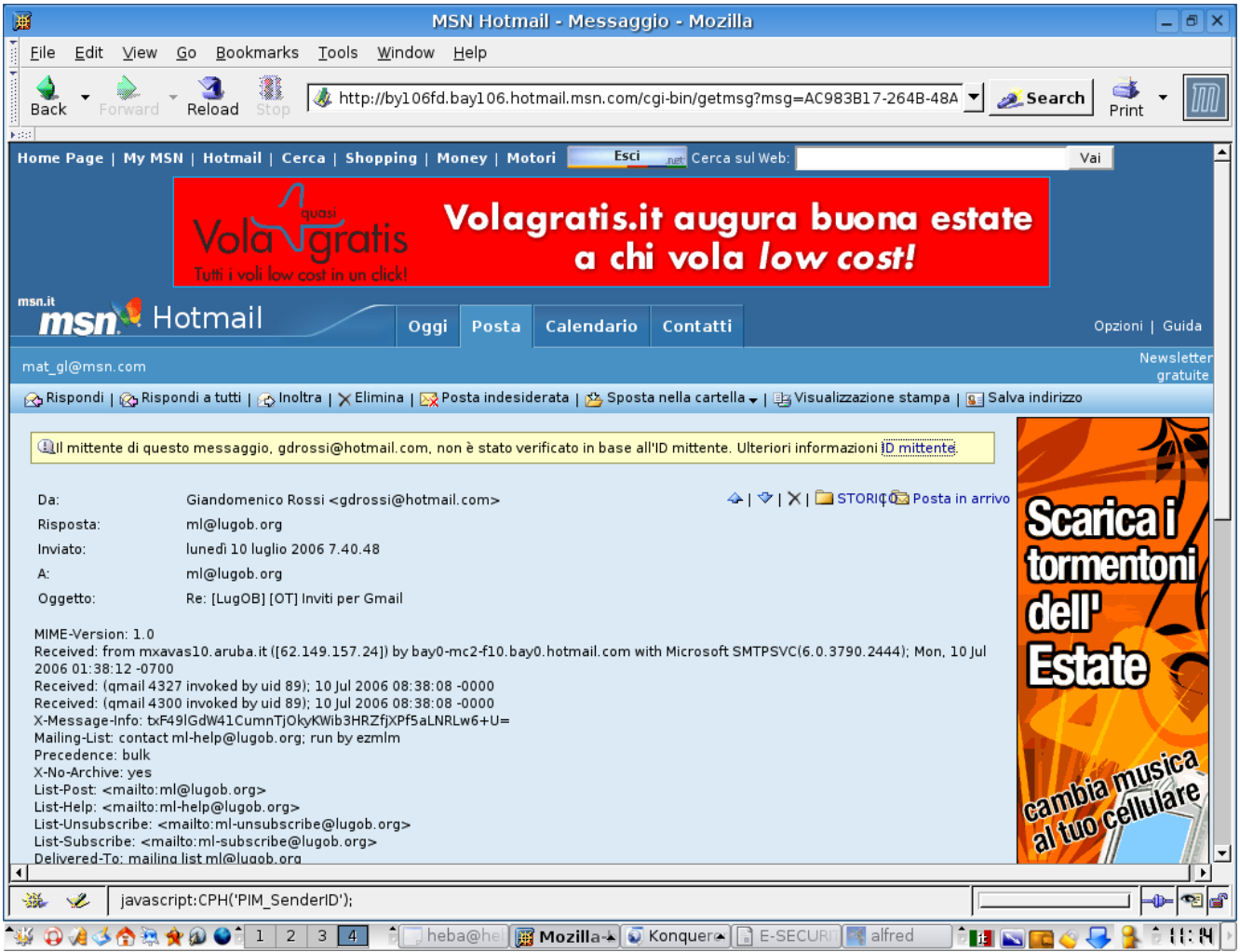
2. La sicurezza delle caselle di posta e dei vari hostes

Ogni host permette di gestire le e-mail internamente ed anche ciò che si può visualizzare e cosa invece no, alcuni permettono di creare nuove cartelle che l'utente può utilizzare secondo le sue esigenze. Ogni host ha una cartella indicata come **spam**, questa è una cartella di default dove finiscono tutti gli indirizzi che sono stati appurati come indirizzi provenienti da persone che fanno spam regolarmente, questo controllo di solito è affidato all'host, gmail ha un pulsante apposito con il quale è possibile segnalare ad un archivio specifico dell'host un indirizzo che effettua spam, con lo stesso gestore di casella di posta è possibile segnalare i casi di phishing, in questo modo prima ancora che le aziende che hanno subito il phishing possano far bloccare il sito da cui proviene la richiesta di verifica delle proprie generalità il link viene bloccato automaticamente dall'host e vengono inseriti questi indirizzi nella cartella spam. Ogni host ha una sua caratteristica che lo differenzia dagli altri, ognuno quindi può scegliere tra tutti gli hostes gratuiti che permettono di avere una casella di posta elettronica quello che più gli piace tra quelli più sicuri in internet. Attualmente i più sicuri in assoluto sono: Yahoo e Gmail, il primo utilizza più controlli nell'invio della posta elettronica soprattutto se il contatto a cui si invia l'e-mail non compare nella rubrica o non è stato salvato come indirizzo sicuro, inoltre è possibile creare degli aliases in modo da mascherare il proprio reale indirizzo e-mail agli occhi di tutti nel qual caso non ci si fidi della persona contattata o si scriva in una mailing list in cui non si conosce la maggior parte delle persone. Sull'host di *Hotmail* è possibile avere una visualizzazione completa dell'e-mail, questo metodo può far visualizzare molte notizie sui riceventi l'e-mail, anche il numero di ip, Hotmail visualizza anche se il mittente dell'e-mail è diverso da quello registrato, per fare un esempio Hotmail utilizza *Server ID*[4] che controlla scrupolosamente che il dominio del mittente sia uguale a quello registrato, come nell'esempio sottostante nella figura 2.

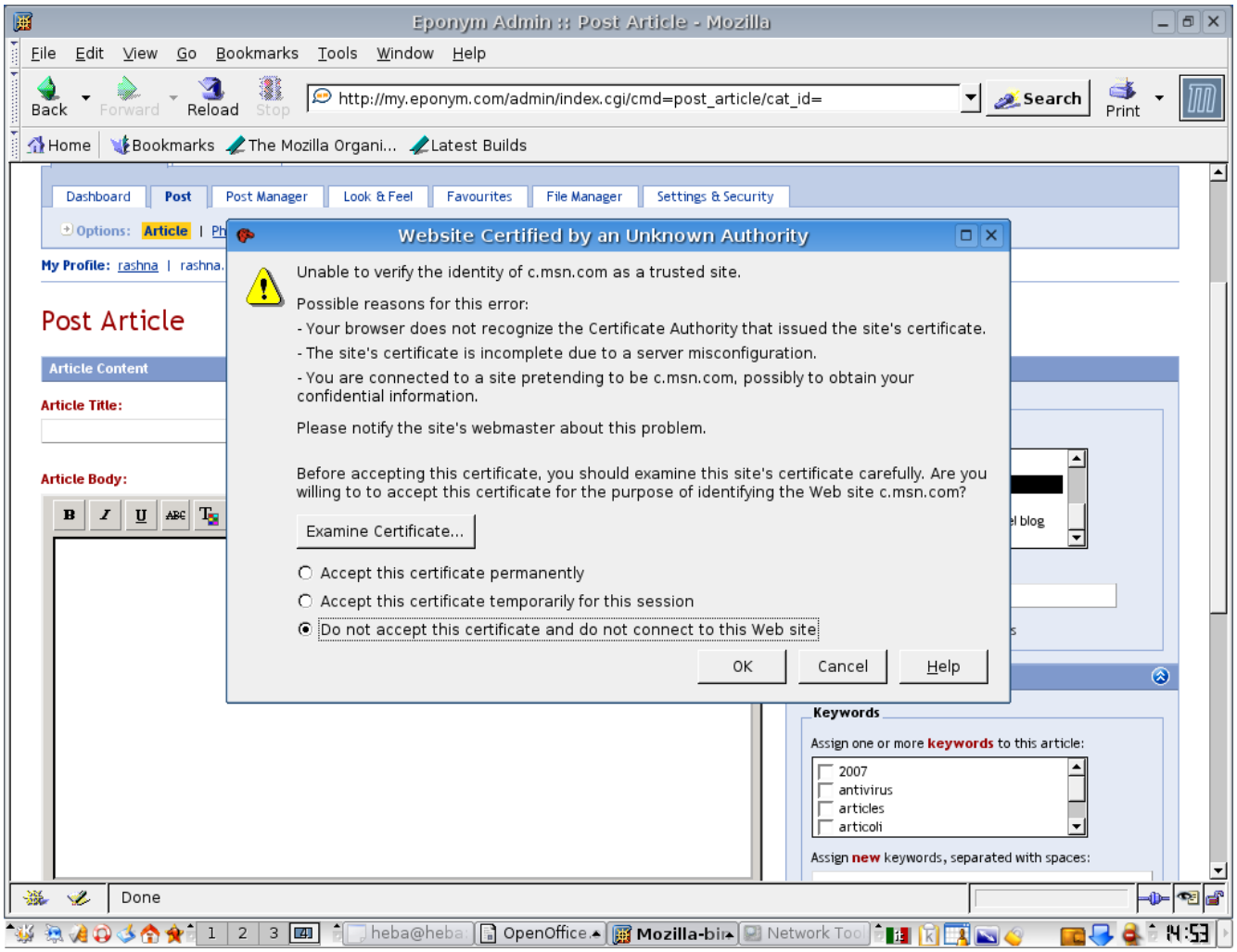
4 per maggiori informazioni visitate questo link http://help.msn.com/(ZmlsdGVyPURIX0ZSRUUmcHJvamVjdD1ob3RtYWlscGltdjEwJm1hcmtldD1pdC1JVCZjdT0mdG10PUhvdG1haWxQSU12MTAma2M9JmZvcm1hdD0=)/Help.aspx?filter=&querytype=keyword&query=PIM_SenderID&fs=1

Figura 2.

come si nota dall'immagine della Figura 2, Hotmail avvisa che il mittente non è la persona che ha inviato l'e-mail, il dominio di appartenenza in questo caso dovrebbe essere **hotmail.com** il Server ID di Hotmail non lo ha riconosciuto come proprio; è difficile che un server non riconosca un suo dominio di appartenenza, diciamo pure che non è possibile a livello di programmazione, visto che di solito le ricerche sono programmate per equazioni precise ed identiche e non sommarie. Quindi non avendo identificato il dominio di appartenenza dell'e-mail invia in testa all'e-mail quel messaggio di attenzione in testa all'e-mail. Questo può accadere nel momento in cui un lamer conoscendo un indirizzo e-mail (che si possono procurare dalle liste di distribuzioni, forum o semplicemente gliel'abbiamo data noi



volontariamente), od usandone uno a caso, ed utilizzando Telnet aggira il server di Hotmail[5] ed invia un'e-mail che però non corrisponde al reale mittente che l'ha inviata, questo può causare in alcuni casi non pochi problemi, perché di solito i lamer utilizzano questo metodo non solo per inviare spam come in passato ma anche per inviare trojan e malware.
In effetti, via e-mail è possibile inviare anche trojan e malware, i più comuni sono i w32, ogni host pubblico però utilizza una scansione online antivirus/malware di TrendMicro che è comunque l'antivirus online più attendibile al momento, ma per poter visualizzare se l'allegato è un malware o un virus con questo metodo è necessario assolutamente guardare la posta elettronica dal web e non scaricarla direttamente sul proprio computer, infatti se si scarica la posta in modo diretto l'host non controlla con una scansione dell'antivirus online, ma questo compito dovrebbe farlo il nostro antivirus che abbiamo installato sul computer.
Un altro pericolo che possiamo correre utilizzando una casella di posta è quello del furto d'identità, un lamer facendo passare la propria chiave crittografica per reale al mail server può ingannarlo e modifica il programma per la verifica della password in modo che rigetti la password inserita, sia che l'errore sia reale sia che invece non lo sia, in quel dato momento vi comparirà un messaggio come nella figura 3 in cui vi si chiederà di autorizzare un dato certificato appartenente ad un sito che sembra uguale a quello del vostro host, ma non è lo stesso, in questo caso il certificato va a caricare il sito c.msn.com.



5 in questo caso, ma potrebbe essere un qualunque altro host. Esistono molte guide hacking in rete su questo argomento, quindi eviterò di parlarne approfonditamente in questa sede.

Figura 3.

Se esaminiamo il certificato come di seguito possiamo intuire che non è il sito ufficiale del nostro host. Come vediamo nella figura 4 e 5, compaiono delle chiavi esadecimali che possono essere tradotte con una semplice tabella ASCII e se andiamo a chiarire ciò che vi è sotto risulterà il nome del certificato posizionato in quel sito, che viene richiamato al posto del certificato reale dell'host.

Figura 4.

Per l'esattezza risulta essere questo sito h t t p : / / c r l . m i c r o s o f t . c o m / p k i / m s c o r p / c r l / M i c r o s o f t % 2 0 c e c u r e % 2 0 S e r v e r % 2 0 A u t h o r i t y (2) . c r l و A h t t p : / / c o r p p k i / c r l / M i c r o s o f t % 2 0 S e c u r e % 2 0 S e r v e r % 2 0 A u t h o r i t y (2) . c r l

Dove vi è Authority Information Access vi è uno script che viene inviato per la richiesta di autorizzazione, al posto di quello ufficiale (fig. 6-7), esattamente: h t t p : / / w w w . m i c r o s o f t . c o m / p k i / m s c o r p / M i c r o s o f t % 2 0 S e c u r e % 2 0 S e r v e r % 2 0 A u t h o r i t y (2) . c r t h t t p : / / c o r p p k i / a i a / M i c r o s o f t % 2 0 S e c u r e % 2 0 S e r v e r % 2 0 A u t h o r i t y (2) . c r t

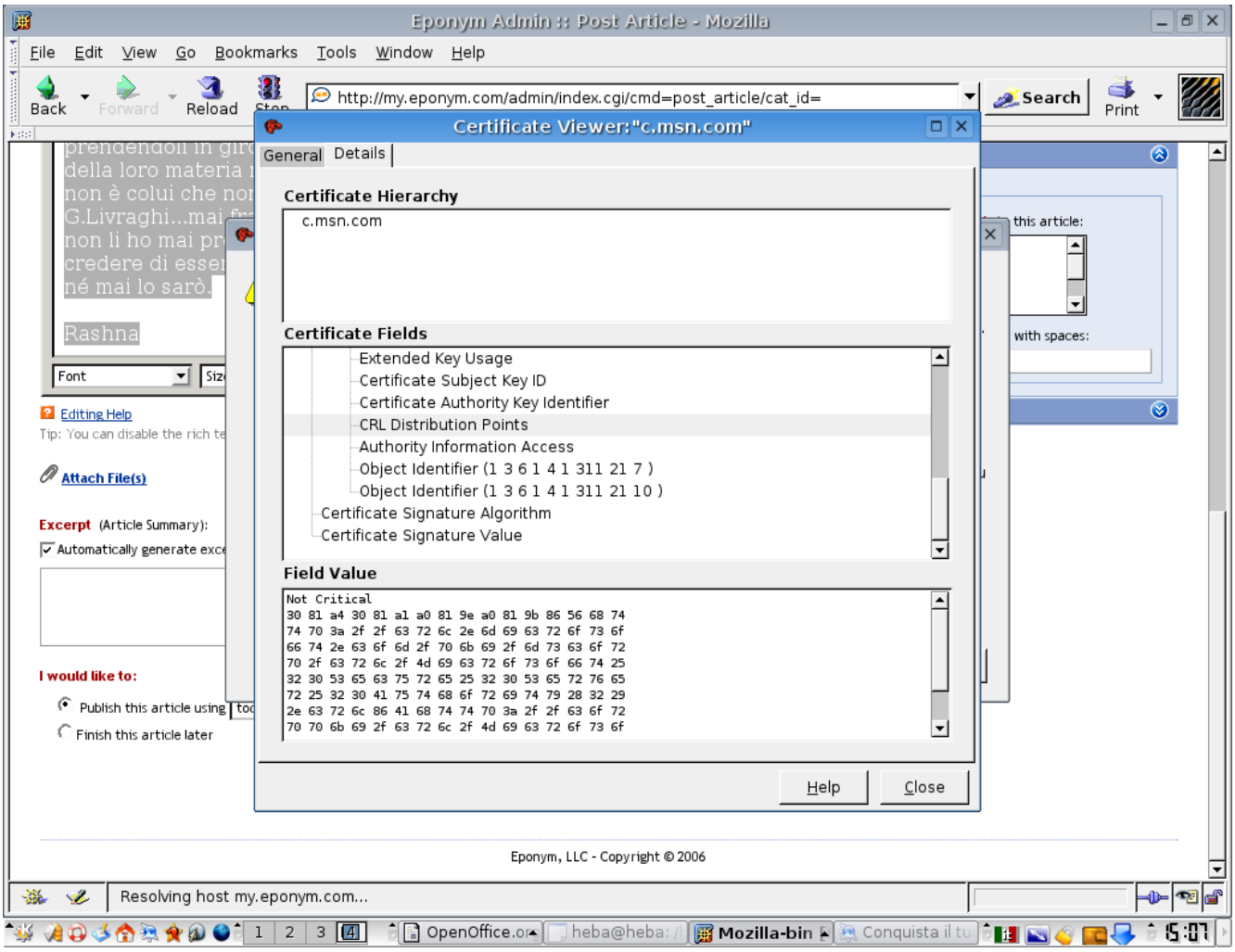
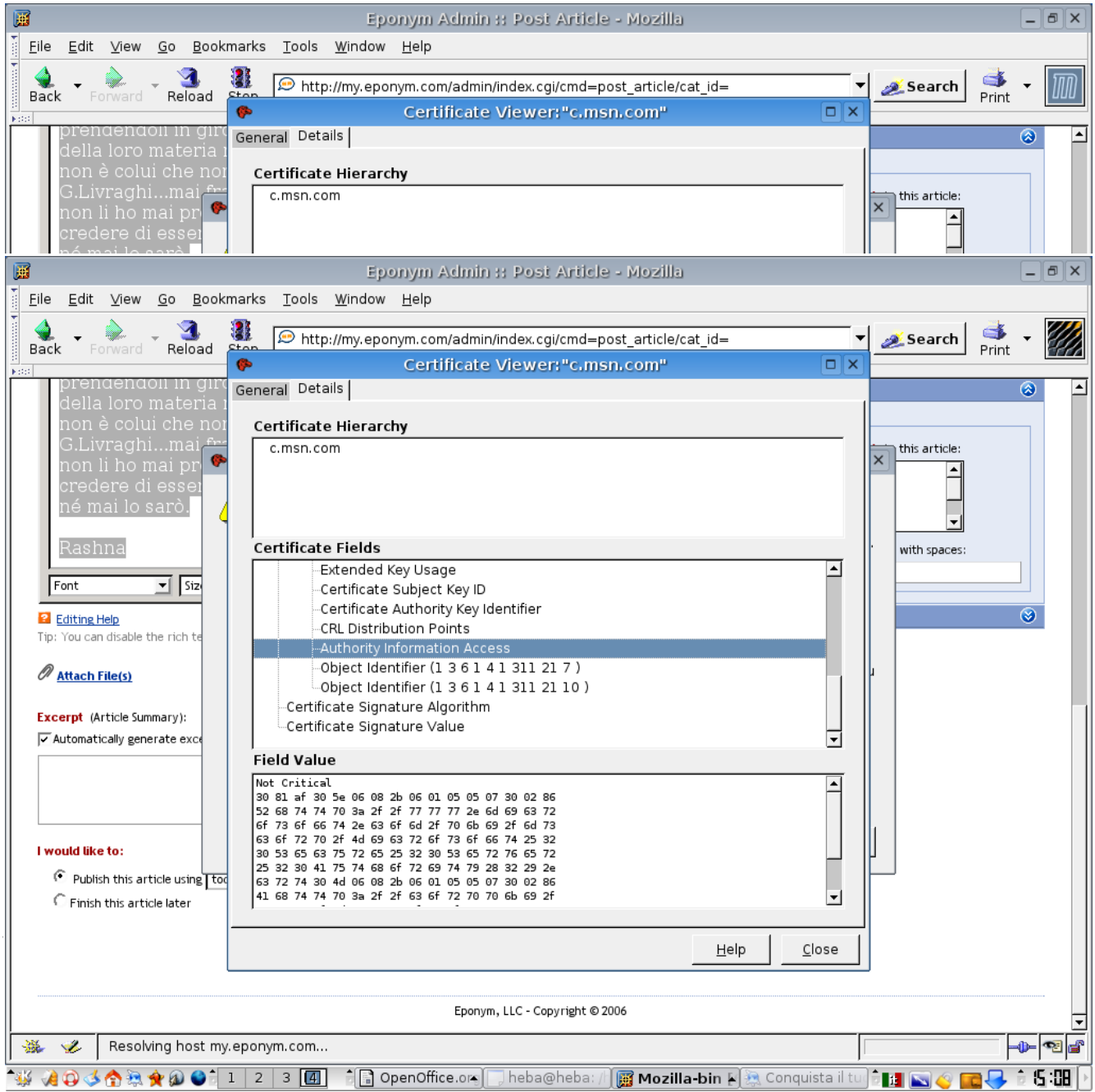


Figura 5.

In *Certificate Authority Key Identifier* vi è inserito in uno script il nome user e del gruppo che verrà utilizzato per fare l'attacco[6] , per chi utilizza Linux saranno nome computer e nome utente il riferimento. Come si può notare quindi il certificato che i lamers cercano di spacciare per vero è nominale e personalizzato, non è quindi possibile che un lamer utilizzi con tutti lo stesso tipo di certificato, questo perché anche a livello di programmazione gli sarebbe impossibile.

Figura 6.

Questi certificati, sono molto pericolosi, questo perché coloro che accettano il certificato con le prime due opzioni rappresentate nella Figura 3, darà la possibilità al lamers di potersi collegare alla propria

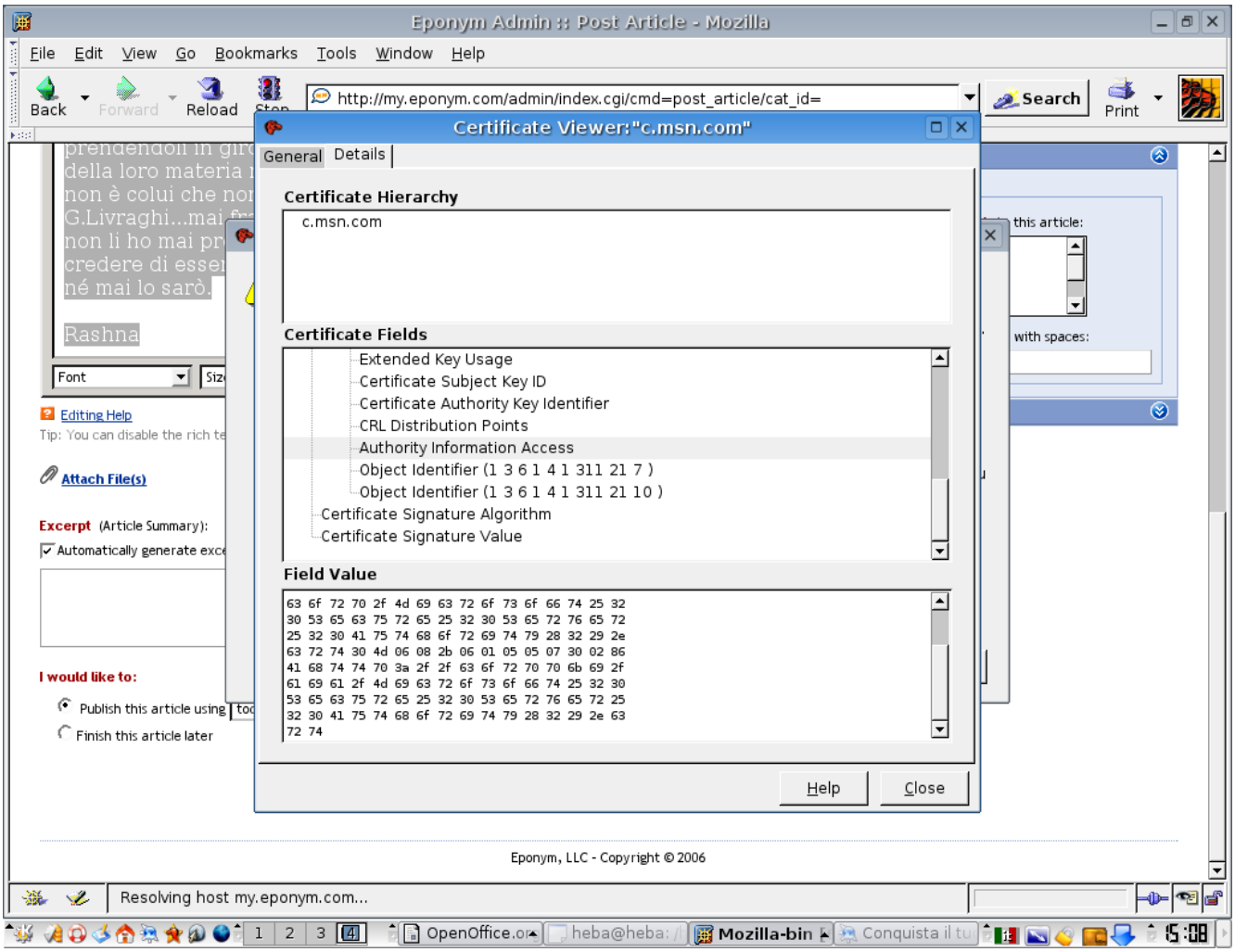


e-mail per tutta la sessione internet se l'opzione scelta è la seconda è per l'eternità se l'opzione scelta è la prima. Nel momento in cui il lamer entra nella nostra casella di posta, potrà leggere praticamente tutto ciò che abbiamo all'interno, le nostre e-mail, i nostri contatti, le cose personali che scriviamo, i forum a cui siamo iscritti, potrebbe impadronirsi di tutte le password e dei relativi siti in cui siamo e potrebbe entrare al posto nostro in detti siti, scrivere una qualunque cosa e spacciarsi per noi. Potrebbe farci apparire soltanto stupidi oppure dei cafoni, dei troll o addirittura farci finire in prigione.
Ultimamente, questo tipo di certificato viene nascosto agli occhi dell'utente in modo da rendere molto difficile la comprensione dell'attacco lamer.
In questo caso, però, l'utente vedrà nella schermata di ingresso un semplice “errore nell'inserimento password”, in realtà è già stato reindirizzato il sito su uno differente per cui all'inserimento di user e password, esse verranno immagazzinate in un file specifico e dirette al lamer che lo ha richiesto.

Figura 7.

Quindi quando vi compare la schermata di ingresso di nuovo dopo aver inserito la password dandovi errore:

a) assicuratevi di non aver sbagliato a digitare.
b) se non siete sicuri, chiudete il browser e riapritelo.
c) se ricapita anche dopo aver riaperto il browser, cambiate browser.



Come proteggersi coerentemente e senza l'ossessione di chiunque contattiamo? semplicemente cercando di utilizzare un po' di buon senso e qualche piccolo accorgimento, quali: non dare il proprio indirizzo e-mail privato, utilizzare servizi pubblici a meno che non si sia certissimi dei firewall e degli antivirus aziendali o personali, controllare prima le e-mail da web poi se si hanno esigenze particolari di spazio o altro si possono spostare le e-mail sul nostro computer, non cliccare su ogni ok che ci compare sulla schermata, leggere sempre bene prima ciò che ci viene proposto, non tutto come si è visto può essere regolare e sicuro.
Nel qual caso si subisca, comunque, un furto d'identità avvisare la Polizia Postale della vostra città.