

# La sicurezza in rete

Premessa:

Libro realizzato principalmente per il neofita, perché le persone più esperte di questo argomento probabilmente conosceranno tutte queste regole e altro ancora.

Ecco, perciò, se ne sapete di più non criticate, perché c'è (e l'ho conosciuta) gente che non sa nemmeno come si accende un computer! Quindi per favore non fate commenti. L'obiettivo di questo (chiamatelo pure "elementare") libro è di trattare i rischi (e i rimedi ai rischi) che si corrono in rete.

# Capitolo 1

## I rischi

Per prima cosa io volevo trattare i rischi che si corrono in rete, addirittura alcune persone neanche immaginano i rischi che vi si possono incontrare. Voi magari pensate che in rete non si possono fare certi incontri, beh, toglietevole dalla testa, ricordate che in rete non si è mai al sicuro, ma noi possiamo adottare certe precauzioni per fare in modo che tali cose non accadano, seguendo una serie di operazioni.

- Aggiornare sempre il computer ad ogni aggiornamento disponibile.
- Attivare un antivirus
- Attivare un firewall
- utilizzare per precauzione un modem router per accedere a internet(facoltativo)
- utilizzare programmi per la navigazione diversi a quelli già impostati.
- I servizi di social network...cos'è Facebook?

Voi direte, ma così tante cose? Non basta avere un antivirus? NO! L'antivirus deve comunque essere aggiornato, e questo comporta anche un aggiornamento del sistema operativo. Inoltre, voi direte, ma perchè un router? Questo lo vedremo più avanti.

Ma adesso parliamo dei rischi che corrono in rete. Una marea. Allora, prendiamo ad esempio un utente che si collega ad internet e i vari passaggi. Allora, un utente normalmente la prima cosa che fa, ovviamente accende il computer. Apre il programma internet

explorer (!) e comincia a navigare, ma intanto, cosa succede? Ecco, allora, tu ti colleghi alla rete, solo che, sì, anche gli altri si collegano alla grande rete chiamata internet, e questa rete da cosa è formata? Da tanti utenti che si sono connessi in quel momento. Quindi, io mi collego alla rete e la rete si collega a me. Ora non pensate che tutti questi computer si colleghino a voi, però è una qualche cosa di simile. Ora noi non preoccupiamoci di questo. Mettiamo che dobbiamo controllare la posta on-line, andiamo sul sito del nostro server di posta elettronica (ad esempio libero, google mail, yahoo. Etc.), ecco, ora che ci siamo collegati a questa specie di portale (quello che si presenta ai nostri occhi), e vedrete tutta quella pubblicità, ecco, avete presente, vi compare una di queste schermate per intenderci:

The screenshot shows the Libero website homepage. At the top, there is a banner with the text "È LA BANCA PER ME, FATTA APPOSTA PER ME!" and "PASSA IL MOUSE QUI SOPRA E SCOPRIRAI IL PERCHÉ!". Below this is a navigation bar with tabs for Community, Blog, Video, News, Mail, Search, and ADSL & Internet. A search bar is present with the text "Cerca:" and a "TROVA" button. The main content area is divided into several sections: "Leggi la tua MAIL" with icons for Mail, Meteo, and Oroscopo; "NEWS" with a headline "Capodanno di violenze" and a sub-headline "Ancora abusi nei confronti delle donne: quattro stupri"; "MAGAZINE" with a headline "Feste, 2 chili in più" and a sub-headline "Tanto cibo e alcolici, e gli italiani ingrassano. Video"; "CHANNELS" with a headline "Ultim'ora Dal mondo" and a sub-headline "Economia Calcio Scienza Finanza Italia"; "COMMUNITY" with a headline "Chatta con i genovesi" and a sub-headline "Ti stanno aspettando Carichi nuove amiche? Scoprire su Trovamic Tributo al Pupone"; "VIDEO" with a headline "Più recenti - Più visti - Primo piano - Più cliccati"; and several advertisements, including "ADSL + telefono + TV 23,28 €/mese PER 12 MESI", "INFOSTRADA Abbiamo ampliato la copertura della Rete!", "BLACKBERRY. INTERNET E MAIL SENZA LIMITI", and "Gioca con Bwin durante le feste! Hai fino a 30€ di Bonus!".

(questo è un riferimento puramente casuale)

Ecco, ma voi siete sicuri che questa pagina sia veramente di quel server? Vi faccio un esempio, se per esempio arriva una mail apparentemente di quel server che vi manda una promozione, un invito, e vi dice di accedere, chi vi assicura che il link che vi daranno nella mail sia quello effettivo della loro originale pagina

di login? Nessuna certezza! Quindi è bene prima dare un'occhiatina, di fatto i server di posta elettronica non inviano questo tipo di mail, in casi come questo è bene segnalare questo alla polizia postale che provvederà a fare gli opportuni accertamenti. Inoltre non cliccate sui banner pubblicitari né tanto meno su quei banner che vi invitano a scaricare suonerie per il cellulare, bisogna ricordare che infatti in rete

non si trovano banner che pubblicizzino un servizio gratuito! Ecco, soprattutto per il cellulare spesso succede che vi siano addebiti indesiderati, inoltre, alcune suonerie vengono inviate in formato .drm, il che significa che sono protette da copyright e non possono essere inviate, e, di conseguenza, copiate!

Inoltre, attenzione agli allegati e-mail! State molto, e sottolineo molto attenti agli allegati e-mail, non sono mai sicuri, e anzi, spesso contengono virus. Cosa sono i virus? E che differenza c'è tra virus e worm? Ecco, sono due cose differenti. Quello che noi chiamiamo virus è praticamente diciamo, spesso uno script che ha un solo obiettivo, danneggiare il computer della vittima, in genere i virus non colpiscono una persona sola, ma si propagano e si moltiplicano attaccandosi ad alcuni file, quindi non aprite assolutamente gli eseguibili e alcuni video sospetti, chissà cosa potrebbero contenere. In genere gli eseguibili sono questi script trasformati appunto in eseguibile con l'estensione .exe. I malware e worm invece che danneggiare, tendono a inviare informazioni personali a una persona in particolare, ossia il creatore del worm. Esso, se il computer della vittima è usato ad esempio per accedere alla posta elettronica, prende principalmente i cookie di questa persona e può addirittura inviarli per e-mail! I cookie sono come dei registratori, che memorizzano gli username e le password dei siti che una persona consulta abitualmente. Quindi attenzione, in rete niente è sicurissimo al 100%!

## Capitolo 2

aggiornare sempre il computer ad  
ogni aggiornamento disponibile

Il computer, per avere le migliori prestazioni, deve sempre essere aggiornato. Perché? Bella domanda. Vi siete mai chiesti perché i professori si informano, gli architetti, i medici si informano sulle novità, perché fanno i corsi d'aggiornamento? Per stare al passo con i tempi? Esatto. Così succede anche ai computer. Un computer aggiornato può informarsi, o, in questo caso, aggiornarsi, sui vari rischi che corrono, e non necessariamente solo quelli riguardanti la grande rete chiamata internet, ma anche riguardanti virus nuovi, etc. Attenzione: i virus non si prendono solo navigando in internet! Ed ecco il motivo per cui bisogna avere installato un buon antivirus anche senza navigare. Ora vi direte voi, bene, come cavolo li faccio questi aggiornamenti? Non vi preoccupate, Windows, il vostro sistema operativo, provvede a cercare gli aggiornamenti in automatico! Quindi niente paura se non riuscite a scaricarli voi. A proposito, gli aggiornamenti si scaricano da internet! Quindi dovete sempre aggiornarli volta per volta, perché un computer non aggiornato che naviga in rete è molto fragile! Se il computer non è aggiornato, prende i virus molto più facilmente, i virus sono danni, quindi rischiate di dover formattare tutto, ovvero cancellare tutto il computer, quindi addio dati importanti, musica, video, album delle foto, etc.

## Capitolo 3

### Attivare un antivirus

Di sicuro avrete sentito parlare di virus e antivirus come una guerra contro un nemico impossibile da sconfiggere, e invece? Cambiate idea, se volete il mio parere, sapete perchè tanta gente è anche, diciamo ignorante, ma non in tutto, solo in informatica? Perchè molte persone vedono nel computer le tenebre, qualcosa di inespugnabile e non alla portata di tutti. Sbagliato. Il computer va solo addomesticato, tutto qua. Ed è proprio quello che vi voglio insegnare a fare. Non dovete pensare che i virus possano essere un nemico che non può essere affrontato, anzi, ora vi dico come fare per rendere questi virus, diciamo, più “innocui”. Poiché molti virus non sono così tremendi, possiamo reprimerli con diversi sistemi, chiaro che invece altri bisogna prevenirli. Adesso che vi ho fatto tutta questa ramanzina voi direte “che palle!”, ecco, quindi adesso chiudo parentesi e vengo al sodo. Un antivirus è un programma che segnala i virus e poi gli annienta se richiesto dall'utente. Ma perchè la gente crea i virus? Ci sono fondate ipotesi che dicono che i potenziali produttori di virus sono quelli che creano gli antivirus! Ma perchè? Perchè se loro creano un virus che il loro precedente antivirus non ha identificato, la gente è costretta a comprare quel nuovo antivirus, e così via. Però l'antivirus, ad ogni modo bisogna aggiornarlo! E perchè bisogna aggiornarlo? Semplice, per lo stesso motivo degli aggiornamenti di Windows. In questo modo infatti, l'antivirus riconoscerà i nuovi virus e sarà capace di eliminarli. Bene, però adesso è giunto il momento che io vi dica quali sono i migliori antivirus, non voglio

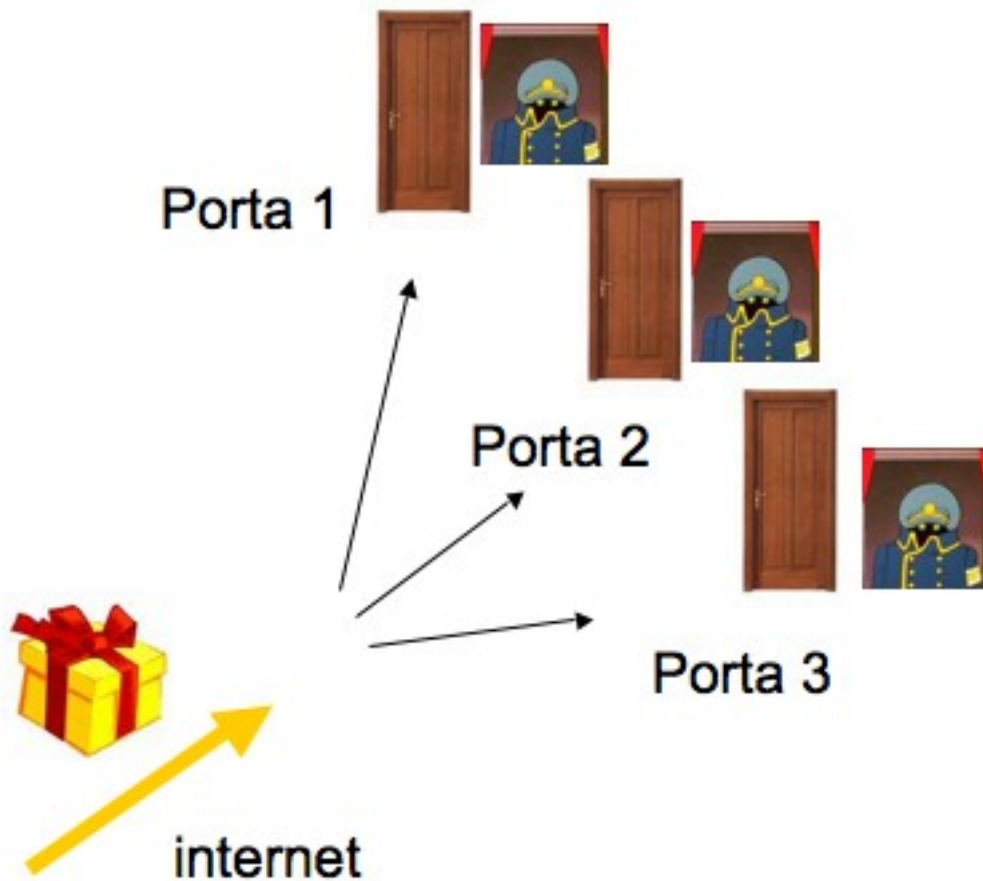
fare pubblicità, assolutamente, ma è giusto che la gente sappia quello che è giusto sapere. A me è capitato che sul mio computer, senza collegarmi a internet, anzi, no, mi sono collegato tipo quattro volte, mi si è installato un antivirus che mi diceva che c'erano circa venti virus. Ma com'è possibile mi sono detto, il computer mi stava da dio, è impossibile, bon, facciamo una contro prova, ma mi sembra strano, dico. Allora, dove ho sbagliato? Ero ancora piccolo e queste cose non le sapevo. Primo, se un antivirus si installa da solo non è un antivirus! E perchè direte voi? Semplice. Il computer, con il sistema operativo Windows, senza antivirus i virus non li riconosce, quindi, questo “antivirus” che si è autoinstallato, non è un antivirus! Poi, dopo questo, questo programma che si spacciava per antivirus ha iniziato a segnalarmi tanti virus, troppi, per solo quattro volte che mi sono collegato, allora cosa ho fatto? Ho preso un altro antivirus, questa volta gratuito (l'altro era un demo), Avast! Antivirus gratuito, fa la scansione anche all'avvio del pc, ma ha un difettuccio, come l'altro “antivirus”, rileva troppi virus, ma perchè? Il computer sta da dio, perchè trova così tanti virus? Semplice, probabilmente non funziona come dovrebbe. Ora, dopo una serie di test, secondo me, Avira antivir è il migliore, poi, secondo me, dovrete scaricare direttamente dal sito della Microsoft, l'antivirus Windows Defender da affiancare ad Avira antivir, in questo modo sarete più al sicuro.

## Capitolo 4

### attivare un firewall

Alle tante regole da applicare per navigare in sicurezza ci aggiungiamo quella di attivare il firewall di Windows. Voi direte, ma cos'è 'sto firewill, firevual, o come si chiama? Letteralmente significa “muro di fuoco”, e fa l'azione di filtrare il traffico dei dati che c'è per la grande rete, ma non solo, anche in quella che può essere la nostra rete privata, che poi vedremo in un capitolo successivo. Ecco, ma un utente cosa se ne fa di questo filtro? Provata a pensare al filtro della piscina. Fatto? Bene. Ora pensate a tanti pacchetti che fanno un via vai per la rete. Il firewall controlla che questi pacchetti siano cosa raccomandabile e che non possa recare danni al sistema, quindi segna anche i tentativi di intrusione. Bene, e quando un firewall trova un tentativo di intrusione, cosa fa? Beh, abbastanza semplice. Dovete pensare che il traffico della rete avvenga come in una casa, quindi ci sono questi pacchetti contenenti dati e informazioni che imboccano porte diverse a seconda di cosa se ne deve fare poi l'utente. Ecco, ora mettiamo che un pacchetto prenda la porta 2, il firewall che in questo caso fa da controllore, in un tempo relativamente brevissimo controlla che questo pacchetto non possa causare danni. Alt! Il controllore (firewall) ha trovato un pacchetto sospetto, viene avvisato l'utente con messaggio di errore, e cosa fa l'utente? Ha due possibilità, dire al pacchetto di fare retro front e chiudere la porta, oppure lasciarlo passare e magari prendersi qualche virus. Per capire più sinteticamente c'è questa figura.

Fig. alla pagina successiva



Voi direte, ma cosa centra questa immagine stereotipata con il discorso? Bene, questa immagine stereotipata, come l'ho chiamata, illustra brevemente quello che ho appena spiegato. Ecco, che si riesce a vedere il pacco regalo che prende il posto del pacchetto dati. Poi le varie porte della casa che in realtà è il computer. Il controllore (firewall) che fa da filtro. Il firewall devo dire che quindi tutto sommato ci lascia abbastanza libertà, perchè ci chiede se siamo disposti a far entrare pacchetti di dubbia identità, invece di non lasciarli entrare e basta. Però in alcuni casi il firewall rompe un po', certe volte, ad esempio nelle chat, blocca (e a me è capitato) la chiamata, o non ti permette di contattare qualcuno, in questo caso dovete scegliere voi: la sicurezza o la chat? A voi la scelta.

## Capitolo 5

### usare un modem router per accedere a internet

Non so se tutti voi sanno che cos'è un modem router, e qual'è la differenza tra l'uno e l'altro. E' abbastanza semplice, in quanto detto in parole povere, un modem permette l'accesso a internet ad un solo computer collegato direttamente, un router invece gestisce il traffico nella rete per più computer, un modem-router praticamente permette a più computer di collegarsi (vedi spiegazione di router precedente) alla grande rete che noi chiamiamo internet. Bene, bene. Ora, perchè si potrebbe mettere anche un modem router per accedere alla grande rete? Sarebbe un ostacolo in più, giusto? Ma se ostacola e rende più complicato il traffico in uscita, ostacolerà anche quello in entrata, giusto? Quindi farebbe da ulteriore filtro, con un altro suo firewall che filtra più pacchetti, e così possiamo essere più protetti e sicuri, difatti, un modem router ci scherma dalla grande rete, esistono però anche modi per scavalcare un router, ma in genere lo fanno professionisti che ce l'hanno con voi. Il costo di un modem router si aggira intorno ai €50, ma anche di meno, però si è molto più protetti. Per rimanere sempre nell'argomento perlerei dei modem router wireless, sono molto comodi per chi ha un portatile e ama usarlo nei vari punti della casa. Bene, questa tecnologia appunto come dice la parola inglese senza-fili, permette all'utente maggior comodità di spostamento, e la velocità non è da meno. Il vostro portatile non ha il wi-fi, ovvero l'opzione hardware senza fili? Nessun problema, basta che abbia una porta USB, e poi, con una chiavetta USB wireless appunto, possiamo sostituire questa opzione hardware. Ok, passo al wireless, ma adesso che chiavetta USB mi prendo? Buona marca a parer mio è quella della D-Link (ancora una volta, lo ripeto, non voglio far pubblicità, solo

consigliare ed indirizzare l'utente a fare il passo giusto). Va bene, ma...quanto costa? Il prezzo non è ne modico ne esagerato, sono circa €20, però dovete pensare alla comodità che questo comporterà. Però, se qualcuno accede alla mia rete a mia insaputa? Niente paura, nelle istruzioni si trova spesso tutto riguardo alla sicurezza e all'installazione del modem-router wireless, ovviamente se non è wireless non serve la password perchè si può accedere collegandosi fisicamente (con i cavi quindi), perciò nessun esterno estraneo alla vostra casa, potrà accedere (eh, lo voglio vedere con un cavo da 10 m). Ma come imposto la password? Per la password, una volta seguite le istruzioni (mi raccomando usate le istruzioni) vi trovate sulla pagina di configurazione del router, girate un po' le pagine, finchè non arrivate a una di questo tipo:

Quick Start **Interface Setup** Advanced Setup Access Management Maintenance Status Help

Internet LAN **Wireless**

Access Point :  Activated  Deactivated

Channel : Undefined   Current Channel: 11

Beacon Interval : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold : 2346 (range: 256~2346, even numbers only)

DTIM : 1 (range: 1~255)

802.11 b/g : 802.11b+g

---

SSID Index : 1

SSID :

Broadcast SSID :  Yes  No

Authentication Type :

---

Encryption :

Pre-Shared Key :  (8~63 characters)

---

Active :  Activated  Deactivated

Action : Allow Association the follow Wireless LAN station(s) association.

Mac Address #1 :

Mac Address #2 :

Mac Address #3 :

Mac Address #4 :

Ora dobbiamo impostare il nome della nostra rete, il tipo di chiave d'accesso e la chiave d'accesso (chiamata di solito password, vanno bene tutte e due), andate nel campo di testo a fianco della scritta SSID e date il nome alla rete. Poi andate su Authentication Type: e scorrete il menu pop-up. Encryption lasciate com'è. Pre-shared key, ovvero la vostra password, digitatela e fate molta attenzione a ricordarvela. Ok, ora siamo al sicuro in questa, il termine esatto è, WLAN, ossia wireless LAN, cos'è invece la LAN, LAN, è l'acronimo di Local Area Network, ossia, per intenderci, la rete locale. Con un semplice modem-router avremo quindi una LAN, con un modem-router wireless avremo la

WLAN. Il prezzo di un modem-router wireless? Circa €60-70-80-90-100, poi dipende dal modello, il prezzo può essere superiore oppure inferiore.

## Capitolo 6

### Utilizzare dei programmi diversi a quelli già impostati

Spesso la gente ignora il fatto che certe volte la sicurezza della navigazione sia compromessa dal programma con cui si, appunto naviga. Usare programmi differenti a Internet Explorer o a Outlook, può portare a maggior sicurezza, come certe volte però può portare scomodità. Usare difatti programmi per la navigazione non legati a un sistema operativo particolare è più sicuro e privato, difatti, i produttori dei sistemi operativi, hanno maggior ragione ad aver interesse a ciò che piace all'utente, ora non voglio fare ipotesi assurde, però, mettiamo che a una persona non piaccia quel browser (=programma per navigare in rete), al momento ha solo quello (ad esempio Internet Explorer), e si mette a cercare Firefox (altro browser), i produttori di questi browser concorrenti (quindi la Microsoft per Internet Explorer), hanno molto, e sottolineo molto interesse ad essere informati sui gusti degli utenti in modo di poterli soddisfare, Firefox (faccio solo un esempio), invece, non ha interessi, poiché da questo non ci ricava niente. Ecco quindi, questa è solo un ipotesi, un ragionamento che ho fatto io, naturalmente, però non ho ancora sospetti fondati. Poi si può cambiare magari programma per la gestione mail, tipo, invece che Outlook Express, Thunderbird. Un'altra motivazione potrebbe essere quella dei virus, quando un virus ti attacca, infatti, va ad insediarsi da qualche parte, quindi anche nel tuo browser, ma...come fa a sapere che browser usi? Non lo sa, si autocopia nella cartella di Internet Explorer e non ti lascia più navigare in pace! Allora, scaricatevi un altro browser (sapete già cos'è? E' quel programma che serve a navigare, in parole poverissime), tipo? Opera, Firefox, anche qualcuno meno conosciuto insomma, basta

che non sia prevedibile per l'insediamento dei virus come in Internet Explorer. In questo modo potremmo essere meno a rischio, poi in rete occorre sempre di stare attenti a tutto, mai lasciarsi trasportare.

## Capitolo 7

### Facebook e il social networking

Fache...cosa?? No, no, è facebook, si pronuncia feisbuck. Ma cos'è?? Un nuovo tipo di croccantini per cani? No, e mi dispiace deluderti, ma stiamo parlando d'informatica. Ma insomma, mi vuoi dire cos'è 'sto face etc.?? Ok, ok, va bene. Allora, Facebook, temuto da tutti gli amanti della privacy...è un nuovo servizio on-line, la mania del momento da quanto definito da alcuni individui (chi?), provoca la dipendenza ad un apparecchio elettronico chiamato computer. Va bene, individuo, non sai ancora cos'è facebook? Mi sembra giusto. Detto in due parole, tu, condividi con amici (e non solo), contatti, preferenze, indirizzi, foto, video, e chi più ne ha più ne metta. E bravo chi l'ha creato...tutto questo ambaradam per che cosa? A cosa serve? “*Serve per tenersi in contatto*” da quanto sento in giro...bella scusa. Utenti di tutte le età...udite! Non cascate in queste furbate. E' una scusa per scoprire cosa ti piace o no...cosa c'è di male? Ah, niente, solo che le multinazionali saprebbero perfettamente come abbindolarti. Anche i ladri ne approfittano, e non parlo di gentaglia, gente senza scrupoli, i criminali informatici. Tramite facebook si può chattare, il che comporta che una persona anche magari a te sconosciuta, si spacci per qualcuno che non è, e in seguito magari cercare, oltre che di truffarti, di insultarti. Ma la criminalità va sempre più diffondendosi, e grazie a questo servizio è sempre più facile per persone malintenzionate, attaccare le persone affette dal morbo detto anche “*ignoranza informatica*”, curabile leggendo questo libro. Quindi, facciamo il punto di questa confusione. Facebook serve a capire i vostri interessi e la vostra vulnerabilità, trasformate poi, queste

informazioni, in denaro a palate da multinazionali che di queste informazioni vivono. Appunto, la scusa è quella di mantenersi in contatto. Schematizziamo:

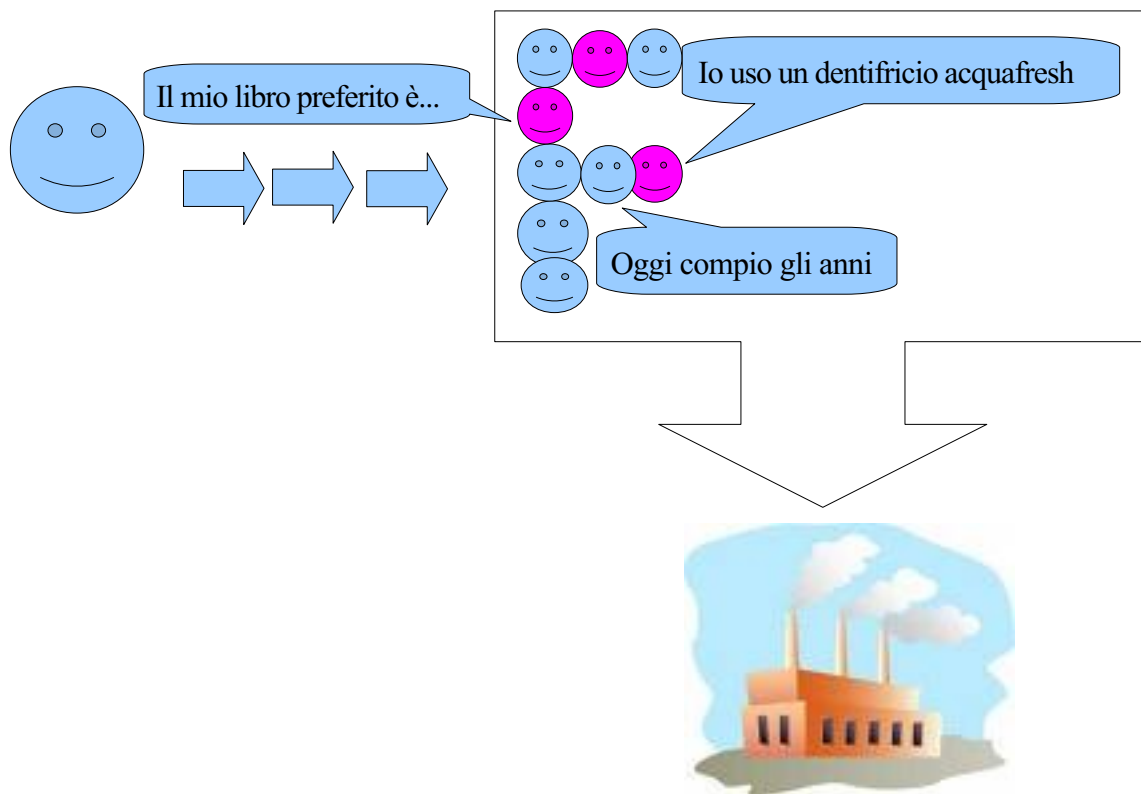


Immagine stereotipata...ma avete capito quindi? In pratica Facebook viene sfruttato per ottenere dati personali di utenti privati. Ma...cosa se ne fa un ladro? In genere le persone più colpite da questo fenomeno sono gli adolescenti, che di solito regalano informazioni personali pur di farsi vedere. Allora, un ladro prima di tutto identifica il soggetto, si stampa le sue foto e guarda dove va a scuola...e fin qui...in seguito, lo segue e cerca di capire anche dove abita. Per il ragazzino e la sua famiglia è la fine. Il ladro si apposterà e spierà tutto quello che faranno, tutte le loro azioni. Quindi, saprà anche se l'allarme sarà disinserito, affermativo? Entra in casa. Negativo? Aspetta ancora. E tutto questo per via di un 13enne che magari voleva solo farsi un po' vedere, un po' notare, che ha messo foto sue, oppure anche

semplicemente per via dei suoi amici, che hanno permesso al malintenzionato in questione di arrivare a lui.

# Capitolo 8

## I cookie

Avete mai sentito questa parola? Cosa centra con l'informatica? Letteralmente in inglese vuol dire biscotti, niente a che vedere con l'informatica, allora, in informatica cosa sono questi cookie? Bella domanda. Una cosa che la maggior parte della gente ignora, è il fatto che tutto ciò che loro digitano può venire registrato, per esempio, vi siete mai chiesti come mai quando magari accedete per tante volte che so, alle mail direttamente sul web (e non sul programma di posta elettronica), accedete direttamente senza dovervi riloggarvi (fare di nuovo il login)? Bene, vi rispondo io. Ci vanno di mezzo questi cookie. Il nostro browser, scrive su dei file di testo (cookie), sotto forma di testo illeggibile, tutto ciò che riguarda il vostro account di posta, quindi username, password, etc. Poi questi cookie vengono rielaborati dal browser che provvede a completare automaticamente i campi di username e password. Accedendo a questi cookie, una qualsiasi persona può esportarli e copiarseli sul suo computer in modo di accedere dal suo computer. Quindi è consigliabile di eliminare questi cookie. Come si fa? Cercate sulla ricerca di Windows (start>cerca) la parola Cookie, aprite quindi la cartella Cookies, ed eliminate tutti i file al suo interno. In questo modo quando un ficcanaso viene a frugare nelle vostre cose non trova diciamo le informazioni più importanti. Esistono poi dei programmi che automatizzano questa operazione.

## Capitolo 9

### definizioni particolari

Ora dovrò parlarvi di alcuni termini di uso comune in informatica, ma che spesso sono errati. Un chiaro esempio è la parola hacker, che noi spesso scambiamo per quella persona che fa del male. In realtà, all'inizio, la parola veniva usata per riconoscere le persone che si impegnavano nel superare un limite che gli veniva imposto (nel campo della tecnologia), il termine italiano che gli corrisponde è *smanettone* e voi vi chiederete, ma cos'è 'sto smanettone, è qualcosa che si mangia? No, è una persona che sta magari ore davanti al computer, e si ingegna, con metodi alquanto particolari, a superare limiti imposti dal produttore. Uno smanettone, spesso non crea danni, bensì fa del bene alla comunità informatica. Un hacker o smanettone è anche chi si crea ad esempio degli script in un linguaggio di programmazione per automatizzare un lavoro monotono. Ora, voi vi chiederete, chi è che crea i virus o comunque si diverte a far del male alla comunità informatica? Il termine americano cracker, è associabile a quella persona, letteralmente significa rompitore. Infatti, queste persone, sono molto esperte di programmazione, e creano danni, ma non solo, spesso rubano informazioni personali (quali codice di conto corrente), in modo da utilizzarli per scopi personali di qualsiasi tipo. I lamer, invece, sono una sorta di cracker meno esperti nei linguaggi di programmazione, che spesso si limitano a creare danni scopiazzando codici usati dai cracker. Difatto qualsiasi persona che abbia una minima conoscenza in materia può diventare lamer, poiché non ci vogliono conoscenze particolari, in quanto, appunto, scopiazzano i codici.

# Capitolo 10

## phishing e altri inganni

Attenzione, il phishing, non significa pescare (poiché quella parola è fishing), bensì è un'arte usata per truffare. Di fatto, il phishing, consiste, per il cracker o lamer (dipende dalle conoscenze, come spiegato nel capitolo precedente), nel diciamo inviare una mail alla persona da truffare, convincendola a cliccare su un link per attivare particolari promozioni. Le mail, apparentemente sono molto convincenti e di grafica pressochè uguale a quella usata dai reali servizi che appunto inviano, o no, questo tipo di mail. Come detto nel primo capitolo, i server ad esempio di posta elettronica tipo Yahoo! Etc. non inviano questo tipo di email. Spesso il truffatore, usante l'arte del phishing, non vuole rubare in alcun modo password ad esempio di indirizzi email, bensì, i codici appunto di conto corrente o carta di credito, per far sì di utilizzare i soldi contenuti all'interno del vostro conto, per fini personali (ad esempio acquistare prodotti per se stesso), oppure per qualsiasi altro inganno a vostre spese (non solo monetarie, ma, udite, anche penali). Se per esempio, come è capitato a molta gente, vi arriva una mail delle Poste Italiane, non è detto che sia della Poste Italiane, difatti è raro che mandi mail promozionali, inoltre state bene attenti a come è scritta la mail, ovvero senza errori, poiché è raro che un servizio li faccia. Ecco, ora, se è vero quello che ci dicono, per verificare, andiamo sulla pagina web del servizio, in teoria, se quella era una semplice truffa, troviamo la “promozione” che ci hanno fatto in prima pagina, se non è così è una truffa, altrimenti, se siete sulla pagina del servizio accedete direttamente, solo lì sarete davvero sicuri che accedendo i vostri dati non vengano rubati. E se mi arriva una di queste mail? Semplice, re inviate la stessa mail alla polizia postale che

provvederà a darvi consigli e ad indagare se necessario, d'altronde, è stata creata proprio per questo la polizia postale, proprio per evitare truffe e abusi in rete.

# Capitolo 11

## sapere chi mette le mani nella vostra rete

Allora, come già vi dice il titolo, voi vorreste sapere chi mette le mani nella vostra rete. Prima però è necessario porsi la seguente domanda. So tutti i termini occorrenti all'uso di questo trucchetto? Ebbene, no. C'è una cosa che non vi ho detto, ma volevo che la imparaste gradualmente, un passo alla volta, ovvero...cos'è un indirizzo IP? Non scandalizzatevi a questa parolona. E' una cosa semplice ma che va capita. Allora, avete presente gli indirizzi delle case? Ovvero via, numero, etc.? Ecco, è la stessa cosa, solo che sono diciamo, numeri...cifre. Allora, un indirizzo IP contraddistingue un computer, è un numero formato da dodici cifre. Un chiaro esempio di indirizzo IP è, ad esempio, questo: 192.168.0.1, ed è naturalmente solo un esempio (come gli altri, del resto), ok, ora, abbiamo questo numerone che ci contraddistingue, ma uno...cosa ci capisce? Allora, diciamo che nella nostra grande rete, che chiamiamo internet, tutti quei numeri vanno a mischiarsi e cambiano ogni momento, no, no, che confusione. Facciamo un passo indietro. Invece, parliamo di questi numeri nella nostra rete che è meglio, se capite che ruolo hanno nella rete siete ben messi perchè nella grande rete appunto succede la stessa identica cosa. Allora, adesso noi parliamo della nostra di rete, ricordate il nostro benedetto modem-router, router, etc.? Ok, allora, noi, con un semplice modem-router o router soltanto abbiamo creato una rete! Allora andate su “connessioni di rete” se avete un Windows, altrimenti su “preferenze di sistema”>”Network” se avete un Apple. Ci siamo fin qui? Visualizza connessioni per Windows. Per Apple, andate su network, Airport, ethernet cable, a

seconda di cosa usate, Airport se usate il wireless integrato, ethernet cable per il cavo ethernet, cos'è il cavo ethernet? Bella domanda. Mi sembra di averlo già detto, correggetemi se sbaglio, niente paura, lo ripeto, in pratica il cavo ethernet è quel cavo simile a quello del telefono solo più largo, non so se riuscite a seguirmi,...perfetto, girate il pc se ce l'avete lì, guardate il retro. Vedrete, se è un pc abbastanza vecchio l'entrata per il cavo del telefono, ora guardate bene, vedrete anche un'entrata per un cavo simile solo un po' più largo, ci siete? Perfetto. Dove eravamo rimasti? Ah, sì, cliccate su una delle due opzioni (vedrete un pallino verde), vi comparirà una finestrella. Ora aspettate. Per i Windows, cliccate con il tasto destro sull'iconcina del metodo di collegamento al modem-router che avete usato, cliccato con il tasto destro? Vi comparirà un menu pop-up, cliccate su “visualizza stato”, vi comparirà un'altra finestra, e vedrete il vostro indirizzo IP nella rete al momento. Fermi lì. Apple, ci siete? Andate da dove eravamo rimasti, sulla linguetta TCP/IP, e anche voi vedrete il vostro indirizzo IP. Bene, ve ne siete fatti quindi un'idea. Adesso, mettiamo che il modem-router normalmente abbia l'indirizzo IP (che ormai conoscete) 192.168.0.1. Bene. Ora andate sul prompt dei comandi, o terminale, oppure shell (Windows, Apple, Linux), e digitate *arp -a*. Ora vedrete che vi compariranno tutti quei numeretti. Ora voi dovete informarvi tramite il libretto delle istruzioni che indirizzo IP ha il vostro modem-router. Se rilevate tre indirizzi IP, quindi, modem-router, voi, e...?? Allora iniziate ad insospettirvi. Attenzione: se voi avete comprato modem e router separati, è possibile che rilevi nella rete, anzi, quasi ovvio, anche il vostro modem. Cos'è un modem, modem-router, etc., l'abbiamo visto in un precedente capitolo.

# Capitolo 12

## Intercettazioni web in casa parte 1

Che strano titolo, no? Ecco, questo capitolo riguarda un'azione illegale da usare solo a fin di bene. Non mi prendo responsabilità a riguardo, in particolare questo capitolo è dedicato ai genitori, che spesso non riescono mai a capire cosa fa lì tutto quel tempo il proprio figlio sul computer, se naviga, dove naviga? Se chatta, con chi chatta? Ecco, allora adesso vorrei dire a tutti quei genitori che quando controllano il figlio questo riduce sempre a icona oppure chiude la finestra come fare per capire se sta navigando sicuro oppure è totalmente scoperto. Innanzitutto dobbiamo avere la nostra rete, LAN o WLAN è indifferente (se non ti ricordi cosa sono guarda un attimo i capitoli precedenti), ovvero dobbiamo avere il nostro bel router. Poi, se vostro figlio (magari cercate di informarvi) usa Msn, possiamo usare il programma Msn Sniffer per Windows però. E per chi ha un Apple o un computer Linux (sistema operativo Linux)? Adesso ci arriviamo. Il secondo programma che quindi voglio proporvi è quello per intercettare i pacchetti sulle varie porte, cosa sono le porte? Lo vediamo nel precedente capitolo, e in quello successivo ancora, vi spiegherò proprio come attuare questo tipo di intercettazioni a fi di bene.

# Capitolo 13

## Le porte

Ebbene, devo assolutamente spiegarvi cosa sono queste benedette porte. Praticamente dice già molto la parola. In pratica sono come delle porte di una casa, solo che ce ne sono molte. Come spiegato nel capitolo dove si parla del firewall, sono delle vie, che possono essere aperte o chiuse. Ad esempio, in una casa, se noi dobbiamo andare, per esempio, in cucina, e in cucina c'è il pavimento bagnato, noi non possiamo entrare. Ecco, ora questo concetto va esportato su quella che è la grande rete chiamata internet. Ora, vi elencherò in una tabella, quali sono le porte più utilizzate.

applicazione	porta
Msn	1080
Connessione alla grande rete	80
vnc	5900
Web chat	6667
Posta in entrata-uscita	995-465

Adesso spero che le persone più esperte mi perdonino, ma certe volte alcuni termini specifici, ad usarli, si crea solamente confusione nel lettore.

Ok, ci siamo? Non so esattamente se avete capito, comunque penso di essermi circa spiegato. Queste sono le porte usate più abitualmente. Voi vi chiedete cos'è 'sto vnc. Cos'è lo vedremo tra poco, altrimenti viene fuori troppa confusione. Allora, queste sono

le porte, quindi non porta 1, porta 2, porta 3, etc. ma queste porte con questi numeri qui. Adesso che spero abbiate capito cosa sono le porte procediamo con la seconda parte della spiegazione precedente.

## Capitolo 14

### intercettazioni web in casa parte 2

Ora che spero voi abbiate capito più o meno cosa sono le porte procediamo con la spiegazione del trucco vero e proprio. Vi ripeto che però è illegale, ma in famiglia può essere anche usato. Bene, adesso scaricatevi il programma gratuito Wireshark. Se non sapete dove trovarlo cercate su Google e lo trovate. Piccolo appunto, se c'è qualcosa se non sapete, se volete approfondire, etc., potete rivolgervi al motore di ricerca più usato, e vi assicuro che troverete lì tutto. Ci siamo, lo avete scaricato? Ora vi spiego (sempre che voi l'abbiate scaricato) cos'è questo benedetto Wireshark. Questo Wireshark è un programma di sniffing (non stupitevi a questa parola, adesso vi spiego meglio). Bene, ora il dubbio che sorge è...cos'è un programma di sniffing? Ottima domanda. Allora, un programma di sniffing è un programma che permette di intercettare i pacchetti dati (vedi figura stereotipata del capitolo trattante il firewall) anche all'esterno (soprattutto all'esterno) della rete. Niente paura, mi sembra che sia un programma totalmente legale, non avete niente da temere se vengono a farvi un controllo.

# Capitolo 15

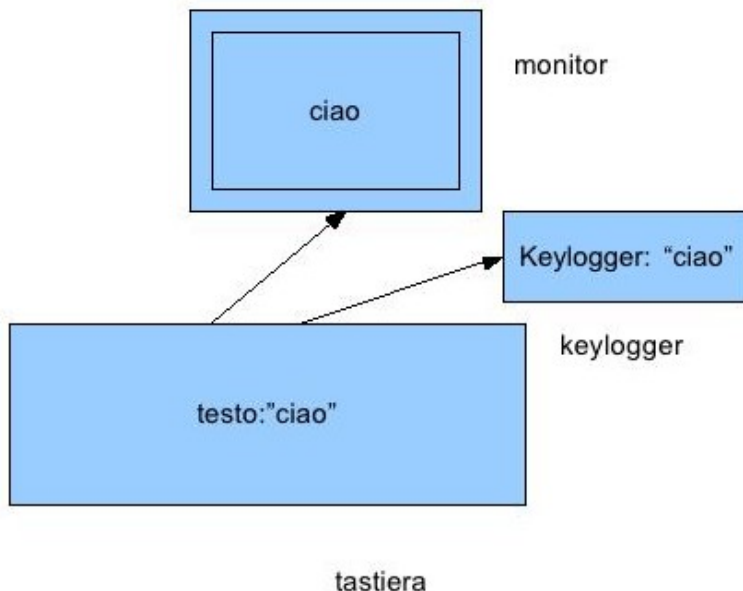
## condivisione delle cartelle in rete

Avete mai sentito questa stramba parola? Cosa sarà mai? No, non è qualcosa che si mangia. Bensì, questa parola dice che i nostri file personali potrebbero essere in pericolo! Magari non esattamente il suo vero significato, ma di sicuro è ciò che intende. Allora, avete mai sentito parlare delle cartelle condivise? No, perfetto. Allora, dobbiamo dire che le cartelle condivise sono pericolose! In pratica noi mettiamo a disposizione degli altri utenti che sono connessi alla rete (LAN s'intende) in quel momento parte del nostro computer, in questo caso le cartelle. Meglio evitare, giusto? Esatto, ma...come si fa? E' proprio quello che devo spiegarvi perbacco, sennò che ci sto a fare io qui? Bene, allora...iniziamo! Clicchiamo sul nostro classico “start”, avete presente? Bene, procediamo, “risorse del computer”, no, non va bene “documenti”, “risorse del computer”!! Scusate la deviazione e la sfogata. Allora, “risorse del computer”, click con il tasto destro del nostro topo, “proprietà”, nel menù a tendina. Cliccate sulla linguetta “condivisione e protezione”, togliete quei segni di spunta (quelle V), e fin qui ci siamo. Ora, andate su “documenti condivisi”, in teoria non dovrebbe esserci nessun documento condiviso. Oddio, c'è?? Eliminatelo.

# Capitolo 16

## Keylogger

Lo so, devo finirlo di dire parolacce. Ma...cos'è un keylogger? Domanda di riserva? Lascia perdere. Allora, qualcuno di voi sa cosa diavolo è un keylogger? Vedo poche mani alzate. Allora lo spiego io. Un keylogger è un programma. Ma non è mica un programma qualunque, è un programma particolare, con il quale una persona può sapere tutto quello che digitate sulla tastiera. Come agisce? Il suo funzionamento è tutto sommato semplice. Praticamente, viene installato da una persona che ha accesso fisico al vostro computer e questo programma registra tutto. Poi, quando questa misteriosa persona torna sul computer, può visualizzare un documento di testo con tutte le parole.



Con questa immagine cerco di rappresentare in parole povere di cosa stiamo parlando. Sì, lo so che sembra fatta da un bambino, però bisognerebbe trovare il modo di far capire a tutti, senza

spiegare la teoria pallosa dove spesso e volentieri non si capisce mai una cicca e ci vuole un dizionario per capire i termini difficili che usano di solito gli esperti del settore. Allora, avete capito? Praticamente noi digitiamo, la parola viene riportata sul monitor e registrata nel piccolo archivio del keylogger, chiamato anche dagli “esperti” database, non so se vi siete resi conto che ho messo la parola esperti fra virgolette, è semplice, molti si definiscono esperti perchè sanno solo scopiazzare codici e usare parole difficili davanti a un neofita e vantandosi delle sue pseudoconoscienze. Pseudoconoscienze, non per tutti, ma solo per, diciamo, i lamer, infatti, sono loro, come prima descritto, che scopiazzano i codici senza capirci magari una cicca. Detto questo, sappiamo che c'è questo programma. Adesso, io non ho provato, ma provate voi a cercare sulla ricerca di Windows, la parola “keylogger”, per vedere se trovate qualcosa. Prima, magari, provate ad installarvelo? E come, non conosco nomi di Keylogger! Google? Cercate sul grande motore la parola “keylogger”, vedrete che qualcosa trovate.

# Capitolo 17

## mettere al sicuro le cartelle

Ci sono diversi modi per mettere al sicuro le cartelle. Il primo della serie è quello di nasconderle...ma bravo, come faccio? Sono qui apposta. Allora, per nasconderle, o le inabissate in qualche cartella di sistema, oppure, togliete l'icona, andate su proprietà, cambia icona, e ne selezionate una dove praticamente non c'è l'icona, e poi, in seguito, la rinominate con un trattino in basso ( \_ ).

Vuoi mettere la password? Lo immaginavo. True crypt dovrebbe fare al caso tuo, se non ti va bene, cerchi su Google (il grande motore di ricerca) un programma per mettere la password alle cartelle.

# Capitolo 18

## controllo remoto

Scommetto che avete sempre sognato di...controllare i vostri amati figlioli quando usano il computer. Come si fa? Mah, sinceramente non saprei. Sto scherzando. Allora, per quest'impresa abbiamo bisogno di un po' di materiale che troviamo, naturalmente, gratuito e in rete. A proposito, per questo giochetto di prestigio, è necessario essere dietro un router, mi raccomando, non siate incoscienti! Non fatelo in rete aperta ad intercettazioni. Allora, vediamo un po' cosa ci serve...mumble mumble...cos'è l'indirizzo IP ve l'ho spiegato...perfetto!

Materiale:

- Un programma atto al controllo remoto, quindi, VNC Server da installare su tutti e due i computer (il controllore e il controllato)
- Un programma tipo VNC Monitor da installare sul controllore
- Una testa che funzioni per non commettere idiozie

Fratello maggiore/sorella che vuole controllare fratello/sorella? Non fatelo. Potrebbe arrabbiarsi. Nota bene: non è una cosa da prendere alla leggera, ricordati che se lo fai a qualcun'altro che non sia tuo familiare, senza il suo permesso, e vieni scoperto, è un reato! Reato=carcere. Il concetto è semplice. Procurati il software? Come no?! Fallo, sbrigati! Hai fatto? Non ancora?? Sbrigati. Ok, ci siamo, installa di nascosto VNC server sul computer da controllare, e guarda che indirizzo IP ha sulle risorse di rete. Ora, è tutto pronto. Spostati sul tuo computer, installa VNC server e VNC Monitor o quello che è. Digita nel campo di testo l'indirizzo

IP del computer da controllare e la password impostata sul VNC server del computer da controllare, perchè avevi configurato il VNC server, vero? L'hai almeno aperto?? Fallo! Prima che torni a casa tuo figlio/a e veda quello che stai facendo sul suo computer. Poi, cerca di fare in modo che si apra ad ogni accensione etc. Ora è tutto pronto, così ti ritroverai a sapere tutto quello che fa lui, pensa che comodità! Senza dover andare poi in camera sua, visto che quando arriverai avrà già ridotto la finestra con quello che stava facendo a icona. Buona fortuna e...attento a non farti beccare!

# Capitolo 19

## Sistemi operativi free

Avete mai pensato, di utilizzare un sistema operativo alternativo a Windows? No?! Bene, invece io vi dico che lo dovete fare...no,...niente ma. Il sistema operativo che vi voglio proporre, non è il solito ubuntu, anzi, linux, come lo chiamano in tanti, e che voi, magari, vista la prima difficoltà, avete lasciato perdere, lo so, è successo anche a me, io non lo volevo usare,...ma questo sistema operativo è differente. Appena sentirete il nome vi stupirete. Per la configurazione, se avete letto tutto il libro a fino a questo punto, non avrete certo molte difficoltà. Il fatto è, che questo sistema è basato sui sistemi linux. Vi ho già detto il nome? No? Ah, già, è vero, il nome è GOS. Ovviamente non voglio fare pubblicità, come sempre, ma questo sistema operativo è troppo bello, inoltre è free...ovvero gratuito, cosa sta a significare? Che se lo piratate da una rete di peer to peer lo fate solo per il gusto di farlo, perchè, siccome è gratuito, non lo piraterete, lo scaricherete soltanto senza infregere alcuna regola, non vi sembra fantastico? Inoltre, per quanto riguarda i virus...siete a posto, non ce ne sono, e probabilmente non ce ne saranno mai, perchè poca gente passa a linux così facilmente, molti dicono che è difficile da usare, e quando ve lo dicono vi consiglio non di mandarli a quel paese...ma...qualcosa di simile, insomma vedete voi. Comunque, secondo me...le cose sono facili da usare solo quando si possono fare solo cose facili, ricordatevelo.

# Capitolo 20

## i motori di ricerca

Allora, immagino che avendo letto questo libro vi siano emersi dei dubbi, magari piccoli, oppure, visto che adesso ci capite di più, volete intraprendere sempre nuove attività con il web. Allora, vi propongo una soluzione, semplice, efficace e, naturalmente, gratuita. Ebbene? I motori di ricerca. Basta saperli sfruttare. Come funziona un motore di ricerca e cos'è? Alcuni pensate che cercano anche dove non dovrebbero, quindi potete stare tranquilli che qualcosa di sicuro trovate. Parlerò parecchio riguardo ai motori di ricerca, perchè è un tema, a parer mio, molto importante, e la gente avrebbe il diritto di esserne a conoscenza, non solo dei vantaggi, ma anche dei rischi. Allora, un motore di ricerca che conoscerete, di sicuro, è Google. Difatto, com'è nato Google? E' nato dal genio di due universitari, ma riguardo alla storia sono confuso anch'io.

I due universitari che fondarono le basi furono:

Larry Page e Sergey Brin. Cosa fecero? Secondo la loro teoria, l'analisi matematica delle relazioni tra siti web avrebbe prodotto risultati migliori rispetto alle tecniche empiriche usate precedentemente. Cosa significa? Lo chiederei a voi. E' difficile spiegarlo. La fonte è Wikipedia. In teoria, quindi, in base alle relazioni tra siti web, viene attuata la ricerca, in pratica sinceramente non ve lo saprei dire. Fu fondato il 27 settembre 1998. Ma parliamo di come usarlo. Mettiamo che tu voglia creare un sito web tutto tuo, hai una discreta quantità di materiale...cerchi “creare un sito web gratis e semplicemente” se sei furbo, o se lo vuoi creare gratuitamente. Difatto cercherò di creare un libro dedicato alla creazione di un sito. Quindi, sui motori di ricerca come, appunto Google, dobbiamo solo cercare

quello che vogliamo fare, e, probabilmente, ci verranno fuori centinaia di tutorial<sup>1</sup> sull'argomento. Bene, parliamo della loro invadenza? Sì dai. Allora, ho visto che Google, ricerca non solo titoli dei post nei blog, nomi di blog, siti, etc. Ma addirittura riesce a cercare nel testo degli articoli. Un bene? Sì, ma anche un male. Da quanto ho scoperto girando in rete, infatti, tale potenza può venire sfruttata da pirati informatici per la rilevazione di falle nei siti, ovvero, per falle, intendo veri e propri buchi, che in alcuni casi si trovano e sono ben evidenti, in altri invece sono magari più nascosti, ma grazie a tali falle una persona potrebbe introdursi all'interno del sistema o server, e rubare tutte le password, criptate o meno (tanto esiste anche il modo di decriptarle), quindi, questa cosa non vi dice niente? Non sentite il campanello d'allarme? Io sì. Il fatto che Google sia troppo invadente, il fatto che qualcuno possa ricercare magari una falla nel nostro sistema, mette paura. Accedendo alla root (radice) di un server, una persona potrebbe avere libero accesso alle varie cartelle, ovvero ai vari domini, e questo comporterà il malcontento degli utenti che si rivedranno sparire le loro cose, e da chi si andranno a lamentare? Dal proprietario del server, che, come risponderà secondo voi? Non potrà sapere, o, dirà al cliente, che vorrà subito essere risarcito, che il sito è stato hacckato e che tutti i suoi documenti sono andati perduti.

---

1 **Tutorial:** insegnamento, guida.

# Capitolo 21

## Trusted Computing

Trust, è un sentimento di fiducia, e non può essere forzato. La fiducia deriva dal fatto che una persona si fida di un'altra, e vi è quindi un legame. Questo concetto di fiducia, è stato riadattato dall'industria informatica. Quindi, se è stato riadattato dall'industria informatica, a cosa può essere riadattato? Ad un chip? Risposta esatta, un punto per il signore la in fondo, un chip. Questo chip, quindi, prenderà decisioni in fatto sicurezza al posto vostro. In pratica, l'utente decide di chi fidarsi, ma la fiducia, è un sentimento che si prova, e non può essere appunto forzato. Quindi, l'industria informatica ha deciso di creare questo chip, che si fida di qualcuno al posto nostro, ma...se è questo chip a farlo...vuol dire che...esatto. Vuol dire che l'industria, di cui siamo clienti, non si fida di noi, che siamo i clienti appunto. Quindi, se loro non si fidano di noi...perchè noi dovremmo fidarci di loro? Questo chip dovrebbe già essere presente dal 2006 su tutti i dispositivi, e, in particolare, sui nostri computer, con un software allegato, che servirà a collaborare con il chip. Il chip, in alcuni casi, verrà addirittura integrato nel processore, così da essere irremovibile. Questo chip, possiamo dedurre quindi che serve a limitare la criminalità informatica. Quindi, impedirà qualsiasi installazione non consentita dal produttore...quindi...programmi craccati? Sognatevi. Nessun sistema operativo potrà venire installato se non autorizzato in precedenza. Questo fatto irriterà molto i pirati, che probabilmente si daranno alla rapina delle vecchiette per strada, quindi, alla fine, l'obiettivo non verrà raggiunto. Nonostante la nuova tecnologia e le restrizioni, il crimine aleggia ancora nell'aria. Per arrivare ad un rimedio del tutto drastico, arriveremo al punto di essere dipendenti dalle macchine, questo è,

probabilmente, il destino che ci spetta. Quindi, io personalmente, e iniziate a farlo anche voi, sono contro il trusted computing.

## Capitolo 22

### navigare restando anonimi

Sì, avete capito bene. No, non è un'offerta promozionale. E funziona? Sì che funziona. Bene, volevo parlarvi un po' delle reti Tor. Cosa sono queste Tor? E' un network, una rete, che ti permette di navigare restando anonimi, questo può essere utile quando cerchiamo qualcosa, quello che cerchiamo viene depositato nei cosiddetti *log* dei motori di ricerca, assieme al nostro indirizzo IP, ma, restando anonimi, sarà quasi impossibile capire chi siamo in rete, e questo può aiutarci moltissimo ad evitare i ficcanaso che si fanno gli affari vostri. Bene, ma dopo questa ramanzina? Ve lo dico sì o no? Sì dai, bon, allora, dobbiamo usare un programma che si conetterà alle reti Tor conferendoci l'anonimato. Il programma da usare si chiama Vidalia, è completamente gratuito, e una volta scaricato, è pronto per essere usato. Attenzione però, ricordatevi di leggere le raccomandazioni sul sito web di Vidalia rima di scaricarvelo, perchè anche per rimanere anonimi ci sono delle condizioni, di diverso tipo. Ad esempio, i plug-in flash, etc. potrebbero svelare il tuo indirizzo IP, e questo vi metterebbe in avanscoperta. Come fare a capire se il nostro indirizzo IP è scoperto e facilmente raggiungibile? Andate sul sito di MostraIP, [www.mostraip.com](http://www.mostraip.com) e lì poi vedete se la gente può capire chi siete. Alternative a MostraIP? Ce ne sono, e in particolare vorrei svelarvi un truccetto che conosco per estrarre l'identità di una persona dietro un indirizzo IP. Allora, per quelli che usano il terminale, quelli che usano Apple o Linux possono, dalla shell o terminale, digitare il comando *whois*, seguito dall'indirizzo IP. Avete Windows? Su Windows questo trucco non l'ho provato, ma ho trovato un metodo alternativo, andate su

[www.ripe.net/whois](http://www.ripe.net/whois), perchè sul sito della RIPE? Semplice, perchè la RIPE gestisce tutti gli indirizzi IP. Bene, quindi, ora trovate sul sito di MostraIP il vostro indirizzo e con whois vedete se siete abbastanza coperti. Per arrivare a nome e cognome dell'intestatario della linea, si deve passare al provider ISP, che non vi darà alcuna informazione a riguardo, poiché è un'opzione riservata alle forze dell'ordine.