LA TRUFFA INFORMATICA – TF1 -

… Eh, no! Non sono un ladro che si è intrufolato furtivamente nei cunicoli di www.francescocaranti.com ! …

Cari amici, ben trovati!
Prende il via oggi, a grande richiesta, una rassegna dedicata ad un altro tipo di consapevolezza … perché ve ne vogliamo trasmettere tanta e quanta ci è possibile fare.
Parleremo di **consapevolezza dei rischi legati ai mezzi informatici**.
I contributi che potrete avere il piacere di leggere saranno pubblicati all'interno della rubrica da me curata '**Piattaforme&Sicurezza**', ma non me ne occuperò personalmente perché … non tutto conosco e ci vogliono tempo e dedizione per raggiungere discreti livelli di conoscenza in tutti i settori che si vorrebbe conoscere. Mi farò aiutare quindi da un 'esperto della truffa': un amico 'misterioso' vi accompagnerà lungo un percorso che affronterà tematiche di grande attualità e di sicura utilità.
Ma … Già! C'è sempre un 'MA' … **Il Guardiano** ed io non vi sveleremo tutti questi segreti per nostra voce, MA ci faremo aiutare da un meraviglioso e caro ad entrambi DEUX EX MACHINA: *Vittorio Malvezzi*.
Vittorio non vi rivelerà la sua identità. In primo luogo perché ciò che conta è quello che ci racconterà; in secondo luogo perché … la vita è più interessante se viene condita da un pizzico di mistero!

Vi lascio un piccolo assaggio dei temi che tratterà e che, a vostra richiesta e discrezione, potranno essere ulteriormente sviluppati:

1. **La macchina**
2. **Il sistema operativo**
3. **Software di lavoro**
4. **Software specifici per le transazioni di borsa**
5. **Software di sicurezza personale**
6. **Reti**
7. **Accesso alle reti**
8. **Minacce delle reti**
9. **Social engineering**

… Quindi? Interessante, vero? E allora, dai! Seguiteci! Vi presento **Il Guardiano**!

Eh, no! Non sono un ladro che si è intrufolato furtivamente nei cunicoli di www.francescocaranti.com! Sono stato invitato dagli amici del Sito a parlare di tutto ciò che concerne **la truffa informatica**. I miei contributi saranno riconoscibili dal codice cifrato **TF** e vi racconterò tutto ciò che avreste voluto sapere, ma non avete mai avuto modo di approfondire. E se avrete domande, dubbi o richieste di approfondimenti potrete scrivere a Vittorio e ad Erika che mi riporteranno i vostri quesiti: sarà un piacere rispondere e approfondire insieme.

Vi aspettiamo!

Erika Tassi e Il Guardiano

TF2 – LA MACCHINA

… Che cosa è una truffa informatica
Come puo' presentarsi
Con chi se la prende
Chi ci aiuta
Che cosa NON fare assolutamente
Che cosa fare in attesa di aver letto tutte le puntate …

Il Guardiano
Ho incontrato il Guardiano in una di quelle sere d'inverno che sembrano fatte apposta per trovarsi con gli amici, a chiacchierare davanti ad un bel camino acceso. E' un giovane uomo, un professionista che fa delle cose molto serie senza perdere un'aria scanzonata che gli porta via una decina di anni. Appartiene ad un corpo specialistico di una Polizia conosciuta, rispettata e molto temuta. Proprio per rispetto ad un lavoro difficile, cerchiamo di non complicargli la vita e rispettiamo rigorosamente la sua privacy. Il suo compito? Oltre a quelli istituzionali, deve controllare i computer e vegliare acciocché i cattivi non riescano a portare le truffe su Internet con troppa facilità. Non è un compito facile, né che si possa pensare di portare a compimento. Devi avere la forza per combattere una battaglia che puoi vincere, ma che non finisce mai. Soprattutto come vedremo ritornare spesso nell'intervista, non devi mai dimenticare che le truffe su Internet non hanno logiche o meccanismi diversi da quelli che ci potrebbero capitare in un'area di sosta di una qualunque delle nostre autostrade. Se non stiamo attenti. E' una precauzione che invita spesso anche noi a rispettare, che si percorrano le autostrade nazionali o quelle informatiche. Lungi dall'essere il tipico smanettone, il Guardiano è un uomo coi piedi per terra, che usa le nuove tecnologie senza farsene travolgere. Ama gli amici, ma piuttosto che su Facebook, che controlla comunque regolarmente, preferisce incontrarli di persona davanti alle fiamme di un grande camino vecchio di molti secoli, sorseggiando una buona grappa ovviamente più giovane, ma solo quel tanto che basta. Tra una chiacchera e l'altra gli ho buttato lì le nostre 6 domande. Ecco le sue risposte, ogni tanto intervengo anch'io, cercando di farlo il meno possibile, proprio per riacciuffare il tema del discorso. Ti ricordo che questa è una fase iniziale, introduttiva. Molte argomenti verranno trattati nel dettaglio in futuro. Parto con le domande.

- Che cosa è una truffa informatica?
Guarda - incomincia sorridendo per non dare un tono cattedratico al discorso – in molti si divertono con gli effetti speciali. I giornalisti poi per mestiere devono intrigare, dare evidenza anche alle cose banali. Enfatizzare. Partiamo invece dalle cose basilari, valide su Internet come nella vita reale. Il reato di truffa viene definito dal Codice Penale che esiste ed è stabile da decenni, molto prima che arrivasse Internet . Del Codice Penale prendiamo la parte che parla "Dei delitti contro il patrimonio mediante violenza alle cose o alle persone. Art. 640 Truffa. "Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032 ." Su Internet cambiano i mezzi tecnici, ma sostanzialmente mezzi, scopi e ambito psicologico no. Soprattutto il complice più coinvolto è di solito proprio la vittima - su questo punto Guardiano tornerà spesso, non come un giudice spietato, ma con accorato coinvolgimento - che spesso pensa di approfittare di una situazione che proprio perché non completamente chiara, potrebbe dare un vantaggio extra, sia pure non completamente eterodosso. Se tutti noi ci comportassimo in modo più onesto e coerente, probabilmente

renderemmo la vita più difficile ai truffatori. Quindi come ci ricorda il C.P. la sostanza non cambia, che ci troviamo su Internet o in un mercatino dove confluiscono merci che arrivano da tutte le parti. Fondi di magazzino e anche ricettazione. Roba buona e specchietti per allodole

- Come può presentarsi?

Prima di tutto mettiamo a fuoco l'approccio al tema sui cui stiamo discutendo. Non diciamo "Truffa su Internet" ma in modo più corretto dovremmo parlare di una possibile Truffa con l'aiuto di un computer. Faccio un esempio un po' al limite, ma tecnicamente ineccepibile: potrei alterare un GPS, dirottare qualcuno che vorrebbe andare a prendere un gelato da Gelato e Caffè e mandarlo alla Taverna dei Sette Peccati, dove mi danno la mezza dopo aver spennato la vittima. Sarebbe comunque una truffa informatica. Come vedi il panorama si allarga notevolmente. Proprio la natura dell'azione dei computer e di tutta la mercanzia che prende il nome di New Media, porta ad ampliare il campo d'azione di chi vuole sfruttarli per intenti criminosi. Prendi ad esempio lo spamming. Di per sé non è necessariamente indirizzato a fini fraudolenti, ma quando ti vengono ad offrire cose mirabolanti, dovresti per prima cosa pensare che se effettivamente fossero vere le opportunità straordinarie, non si vedrebbe la ragione di doverle offrire ad un così enorme numero di indirizzi. – Intervengo a ricordare al Guardiano la massima saggia e mai abbastanza ascoltata, che gira sulla Rete: <Se qualcosa sembra troppo bella per essere vera, molto probabilmente vera non è> . Lui sorride ancora e continua – Verissimo, ma non esageriamo, mi raccomando. Non facciamo di tutte le erbe un fascio e non precludiamoci ogni offerta. Internet a volte serve proprio per sfruttare occasioni che seguendo i tradizionali canali di distribuzione, non sarebbe possibile ottenere. Una volta ancora riportiamoci al mondo reale: anche qui ci sono offerte speciali, per esempio nelle stagioni dei saldi, di cui sarebbe un delitto non approfittare. D'altra parte proprio in queste occasioni ci sono anche i birichini che ci marciano dentro e guarda caso il nostro Corpo veglia per beccare gli abusi e le tentate truffe. L'unica vera differenza tra truffe su Internet e quelle nel mondo reale, sta nei grossi volumi che sono veicolati tramite i new media. Quindi percentualmente sui grossi numeri è possibile che in valore numerico aumenti anche la quantità di truffe. E' quello su cui contano i malintenzionati.

- Con chi se la prende, quale la vittima tipo?

Chi è la vittima tipo ? mi spiace deluderti. Possiamo esserlo tutti. – e qui diventa categorico pur senza montare in cattedra, vuole esser sicuro che riceva il messaggio – La vittima spesso diventa complice e finisce per meritare in qualche modo quello che le capita. Ti faccio un esempio, sempre nella vita reale. – offro me stesso con notevole spirito di sacrificio che spero apprezzerai – Si, l'esempio che mi hai fatto prima sulla tua esperienza londinese calza. Se nonostante ti abbiano detto che la circolazione è dalla parte sbagliata, che quando scendi dal marciapiedi devi guardare dall'altra parte … tu continui a guardare a sinistra, beh rischi di finir sotto un veicolo. Magari non te la sei cercata, hai la scusante della forza dell'abitudine o di non so che altro. Resta il fatto che non hai rispettato le regole del luogo dove ti trovavi. Se poi per fare una furbata o per pigrizia, attraversi lontano dalle strisce pedonali o dal semaforo, allora caro Vitt si che te la sei cercata. Tentiamo dunque di spiegare e inculcare le regole che vigono nel mondo in cui ti trovi in quel momento. Vuoi proprio una categoria a rischio ? Mediamente chi usa il computer "costretto", magari per lavoro e non lo usi con attenzione e interesse. Chi si muova sulle strade di Internet in modo colpevole, cercando di approfittare di quella che sembra una allettante furbata, o in mancanza di un certo tipo di conoscenza elementare, è disarmato. – intervengo per far capire che il messaggio è arrivato forte e chiaro. E' come se tu accedessi ad Internet senza installare un Antivirus e un Firewall ? – Si, ma non dimentichiamoci anche le responsabilità che non gravano sulla vittima designata. Nella vita quotidiana se qualcuno salta su un'auto senza patente, nell'andare in giro trova una serie di grosse difficoltà oggettive. Non conosce i segnali stradali e per non essere a suo agio alla guida ha uno stato d'ansia e tensione che diminuiscono la sua lucidità e capacità decisionale. Proprio per questo la società, per proteggerlo e proteggersi, ha messo delle regole fra cui la necessità di dotarsi della patente di guida. Se tu vai su Internet e fai uno sfascio, non gliene frega niente a nessuno. Tutt'al più sarai "bannato" cioè ti impediranno l'accesso a qualche sito. Quindi io, proprio per preservare la splendida libertà che ancora si vive in Rete, suggerisco a chi meno ha

dimestichezza con computer e accesso alla Rete, di usare questi due mezzi in modo ricreativo. L'effetto ludico porta a smitizzare certi strumenti riportandoli al loro rango di mezzo per ottenere qualcosa. Dobbiamo imparare a vivere il computer con naturalezza, magari con l'aiuto di un amico, un parente o sfruttando tutte quelle opportunità spesso gratuite che offrono organizzazioni pubbliche o private senza fine di lucro.

- Chi ci aiuta?

Rischio di essere ripetitivo, ma il primo aiuto devo darmelo da me stesso. I Sistemi Operativi sono a livello di utente medio, però devo imparare a usarli, senza drammi e senza pensare che si tratti di roba trascendentale riservata a marziani o a giovani geni. Chi può darci una conoscenza di base ? Si ci sono le scuole di cui abbiamo appena parlato, ma non aspettiamoci che ci diano una ricetta valida in assoluto. Come abbiamo detto cinque minuti fa, anche un adulto apparentemente senziente cui abbiamo insegnato come si attraversa la strada in Inghilterra, se non ci mette del suo poi va incontro a guai. Molto grossi a volte. Si va a scuola per imparare ad accedere con naturalezza e facilità alle informazioni, cioè imparare il metodo per utilizzare nel nostro caso un software e un hardware. I mezzi per il mondo virtuale. Ma utilizzarlo in modo virtuoso è un'altra cosa – concordo e intervengo per ricordare il mio personale, assoluto e finora insoddisfatto bisogno di una scuola che mi insegni il … buonsenso – Tutto ciò non è impossibile e neanche poi difficile in modo insuperabile: si tratta di compiere un percorso, come se ne fanno tanti nella vita di ogni giorno. Non esiste una scuola di Internet, come non esiste una scuola di vita. – ammenocchè non si parli di filosofia e religione, intervengo io - Si certo, ma allora andiamo fuori tema. – risponde sogghignando il Guardiano – Creatività e tecnologia non sono un male di per sé, ma caso mai come ne facciamo uso.

- Che cosa NON fare assolutamente?

Ti ricordi quel che ci dicevano da piccoli ? Non prendere caramelle dagli sconosciuti. Non farti agnello, chè lupo ti mangia. Internet è sempre il Pianeta Terra, non ci trasferiamo su Marte. Non esagerare d'altro canto in senso opposto e portarsi dietro sempre la paura di tutto. Non rinunciare alla privacy e non fornire i nostri dati privati, così come non daremmo carta d'identità, codice fiscale e carta di credito al primo che passa per la strada. Men che meno fornire i nostri dati a chi dovrebbe già averli, se fosse davvero chi dice di essere. Caso tipico chi spacciandosi per un ente finanziario tenta di rubarti i codici d'accesso ad un'area privata, con la scusa di un controllo. Non ci sono regole fisse per Internet, come non ci sono regole fisse per il buon senso. Non fare nulla di cui potremmo pentirci. Non facciamoci confondere dal mezzo tecnico che stiamo usando e con il quale dobbiamo dunque acquistare confidenza. Non dimentichiamo quello che abbiamo imparato a scuola, dai genitori o con una dura esperienza di vita personale. Non credere ai guadagni facili, sia che vengano offerti all'angolo di una strada col gioco delle tre carte o sul computer quando ci offrono di far transitare soldi sul nostro conto guadagnando senza fatica. Quindi assolutamente NO a ricevere e trasferire fondi, specie su banche estere.

- Che cosa fare allora in attesa di aver letto tutte le puntate?

L'aspirante vittima, o meglio chi non voglia aspirare a questo ruolo, dovrebbe apprendere dalle sue esperienze e anche da quelle di altri. Se qualcuno legge le mie parole, mi sembra già stia iniziando quel percorso di cui si parlava prima. Chi cade dalla bicicletta mentre impara a pedalare e non risale in sella, non fa tesoro dell'esperienza. Sviluppare il mio senso critico. Una volta c'era chi diceva: "è scritto sul giornale, quindi deve essere vero". Poi abbiamo tutti imparato che magari in buona fede, il più delle volte per fini ben precisi, anche i giornali possono non contarla su giusta. Stessa cosa in Internet, perfino la benemerita e meravigliosa enciclopedia Wikipedia non dovrebbe esser presa sempre come oro colato. Non interamente e a priori. Quando si può, verificare sempre seguendo un'altra via. Se mi chiedono i dati di accesso al mio conto, calma e gesso. Prendo il telefono e chiamo la banca o la Posta, o faccio un giro e vado a parlare di persona. Ci farò anche la mia bella figura, quella di uno o una che non si fa imbrogliare e che sa usare correttamente anche i moderni mezzi tecnologici. Informarsi e tenersi aggiornati. Come leggo il giornale per le notizie di uso pratico, così

accediamo ai siti di Internet che ci tengano regolarmente informati su quali siano le truffe più alla moda.

Grazie Guardiano! Ti aspettiamo qui le prossima volte per continuare ad essere informati!

Vittorio E. Malvezzi e il Guardiano

TF3 – IL SISTEMA OPERATIVO

… E' una notte scura e tempestosa da far impazzire anche Snoopy quando incontro il Guardiano …

Mi sorride come sempre, ma gli occhi arrossati tradiscono stanchezza. Scopro che negli ultimi giorni il dormire è stato un optional per lui. Li ha passati saltando da un aereo all'altro per occuparsi di computer e dei loro problemi in mezza Italia. Subito parte un'amichevole schermaglia su chi-inviti-chi, ma presto devo arrendermi alle conoscenze tecnologiche superiori, alla simpatia e alla forza di una prorompente gioventù. L'invitato sarò io, cerchiamo almeno di non fare l'Invitato di Pietra. Cominciamo bene! Claudio, Chef pluripremiato e proprietario della Trattoria Cacciatori ci riserva una sala tutta per noi e un menù da leccarsi i baffi. Piccolo antipasto di pesce caldo con gamberi all'armoricaine à la Chef, con bianco frizzante morbido per sposarsi alla salsina dei gamberotti. Poi facciamo sul serio: affrontiamo decisi del maiale in agrodolce con scorze di arancia caramellate e flambèe con un bel Nero generoso e rotondo. Chiudiamo con formaggi locali con miele e un semifreddo di torrone (N.B. mica il solito torroncino prefabbricato) con pere cotte strafugnate nella salsa di cioccolato. Caffè e basta perché faremo i conti con la grappa extravecchia tra poco a casa.
Qui giunti, pochi passi graditi come dopo-cena, tutti concordi rinunciamo al camino già pronto per non rendere più penosa la nostra lotta contro il sonno. Senza pietà, parto con le domande al Guardiano.

Che cosa si intende per Sistema Operativo ?

Il S.O. è un software – *mi risponde cercando di partire dalle cose elementari per fare chiarezza* – cioè un insieme di istruzioni scritte da esseri umani, e quindi come tali soggetti a possibili errori, istruzioni che servono a gestire l'Hardware, termine che tradotto alla lettera può suonare come "Ferraglia" o Ferramenta e si riferisce alla parte solida del computer: la macchina con le sue diverse periferiche. Compito del S.O. è quello di far funzionare sulla macchina altri software di uso specifico: gestione testi, database, browser ecc. Abbiamo parlato di possibilità di errori non a caso, perché questi costituiscono una potenziale vulnerabilità a potenziali attacchi. Esistono naturalmente tecniche specifiche per scrivere correttamente i programmi, ma i codici sono tali e tanti che gli sviluppatori possono commettere errori o lasciare dei buchi. In inglese tutta sta roba la chiamano "Bugs" per un motivo divertente. Il primo caso famoso di errore di un computer viene fatto risalire all'introduzione nel computer di una sventurata farfallina, bug appunto. Da allora i pasticci nei programmi vengono anche chiamati così. Dunque non esiste un software perfetto, ma tutti sono perfettibili. Fra l'altro chi sviluppa virus ma soprattutto gli Hackers, finiscono con aiutare indirettamente i programmatori. Un attacco segnala una falla e quindi rende possibile una correzione. Per la particolarità del S.O. di essere alla base del funzionamento del computer, minare il S.O. vuol dire minare ogni operazione che viene compiuta grazie a lui. La più palese evidenza che forse abbiamo un ospite indesiderato, un malware cioè una porcheriola elettronica che abbia corrotto un file, è la improvvisa e ingiustificata lentezza della macchina. Allarme, il S.O. incomincia ad essere forzato a fare suo malgrado qualcosa per cui originalmente non è stato programmato. D'altro canto un Antivirus "perfetto" non esiste, il suo sistema di aggiornamento non è prevedibile e quindi la loro reattività si muove in modo non

omogeneo. Oggi può essere più avanti l'AV Pinco e domani invece l'AV Pallino. Neppure si possono installare più antivirus sulla stessa macchina, perché entrerebbero in conflitto. I S.O. più noti per personal computer sono 3: Windows, Mac e Linux.

Come Impatta con una Possibile Truffa?

Ogni software ha dei bugs o almeno dei talloni di Achille di cui possono approfittare malintenzionati o Hackers. Faccio questa differenza perché a volte questi buchi vengono scoperti non da criminali, ma da quelli che vengono chiamati Hackers, una roba diversa ! Questi sono degli esperti che hanno una loro etica che il più delle volte rispettano rigidamente. Un'etica forse anomala ma accettabile, ben diversa da quella dei Crackers (i Rompitori, devastatori) che già scivolano nel crimine. Come abbiamo visto, chi scopre e segnala, magari per farsene un comprensibile vanto per la propria abilità tecnologica, fa un grosso servizio allo sviluppatore e a tutto il mercato. Cioè anche a me e a te. Vengono molto considerati nell'ambiente tecnico, una volta ancora ti riporto al mondo reale. Il più grosso errore che un utente di Internet possa fare, è quello di credere che si tratti di un mondo ideale avulso dalla realtà dove valgano regole non ben chiare ma diverse dal mondo quotidiano. Internet, e non lo ripeterò mai abbastanza, è si un mondo parallelo, ma composto da umani cioè io e te che anche lì ci comportiamo come facciamo tutte le mattine. Che si esca ad affrontare la pioggia per andare in ufficio al mattino o che ci si colleghi a Internet, siamo sempre noi. Quindi parlando di comportamento etico da parte di un tecnico, sia Hackers o invece criminale, è come se ti dicessi che un ottimo meccanico può ripararti l'auto in quattro e quattr'otto addebitandoti la giusta tariffa per le sue prestazioni. Oppure può refilarti un bidone e per una candela sporca chiederti la revisione del motore. Anche questi fanno danni e ti truffano, la logica è sempre la stessa, cambia solo l'ambiente. Non ti far confondere solo dal fatto che cambia il mezzo di comunicazione, chiacchere a quattrocchi o chats sono sempre e solo un mezzo con cui gli umani comunicano. In entrambi i casi possono darti calore umano o refilarti un bidone.

Non sono uno <smanettone>, cosa faccio ?

Certo, capisco. E' la prima obbiezione che mi fanno tutti i non professionisti. Però … per andare in auto mica devi essere un meccanico specializzato, no? D'altra parte un minimo di cultura in materia devi averla, è quello che ci impartiscono quando prendiamo la patente, seppure in modo embrionale. Torniamo al discorso già affrontato circa l'informarsi. I modi come abbiamo detto sono diversi, non necessariamente costosi e possono anche essere divertenti e aggregativi.
Ne vale la pena, credimi. Un primo suggerimento, proprio per non fermarci nel generico, è quello di fare gli aggiornamenti di sistema operativo e programmi vari. Mi chiedi come si fa ? E' abbastanza semplice, sostanzialmente ci sono due sistemi: l'automatico e il manuale. Automatico è quando utilizziamo una funzione dedicata e fornita direttamente dal produttore del S.O. Microsoft per esempio ti dà questa possibilità, si tratta solo di configurare la sezione della versione in uso, mettendo qualche flag, il segno di spunta, nelle caselline. Il sistema manuale è un filino più lungo ma forse ancora più semplice. Ti colleghi al portale del produttore del software e cerchi l'ultima versione. Quasi tutti, avendo la convenienza a fidelizzare il cliente, ti offrono l'opportunità di essere informato quando uscirà la nuova versione. C'è un ulteriore modo, una miscela dei due, e si tratta di usare dei programmi specializzati che spazzolano il tuo computer alla ricerca dei "drivers" e controllano gli aggiornamenti. Alcuni sono anche gratuiti: http://www.geekissimo.com/2008/07/21/double-driver-salvare-e-ripristinare-tutti-i-driver-in-due-click/ Ovviamente non devi esagerare o preoccuparti troppo. Se non hai innescato degli automatismi, cosa altamente consigliata almeno per il S.O., un controllo generale ogni 6 mesi/ 1 anno bastano. Senza contare che se ogni tanto senti la necessità di fare le pulizie generali e porti a formattare il disco fisso, in quell'occasione ti aggiorneranno automaticamente anche i drivers.
Poi sempre per fare degli esempi, utilizzo delle protezioni automatiche tipo Antispyware, Firewall, AntiVirus. Purtroppo devo imparare ad usarli. Non è poi così difficile: basta frequentare qualche sito e leggere qualche giornalino di settore. Nel dubbio un trucco usato proprio dai professionisti, è quello di testare la stessa situazione su un'altra macchina, tua o di un amico compiacente. Tieni presente che in casi disperati, quando tutto sembra improvvisamente non funzionare più, c'è una sicura via di fuga e salvezza. Si chiama "Punto di

Ripristino" è qualcosa di magico, tipo quando da bambini si voleva fermare tutto e ricominciare da capo e si gridava <a-rimortis>. Cerco di spiegare per sommi capi. Il computer qualche volta fa anche delle cosette simpatiche, tutto da solo. Sempre che i programmatori ci abbiano pensato prima e lo abbiano adeguatamente preparato. Il punto di ripristino è una situazione di fatto che viene "congelata" e salvata ad un momento X e che in caso di necessità consente di tornare indietro e recuperare tutto come si trovava in quel momento. Se oggi mi accorgo che qualcosa non funziona più come vorrei e soprattutto come funzionava solo due o tre giorni fa o che so, un mese fa, cerco il punto ripristino più vicino a quel momento e lo recupero. Si può fare anche senza gridare arimortis ! I punti vengono creati automaticamente dal programma ogni tanto o quando chiedi di fare un'azione che secondo il programmatore potrebbe comportare dei rischi. Puoi anche decidere tu di crearne altri e scegliere il momento in cui farlo. E' una grossa chance, un salvagente cui anche i professionisti ogni tanto ricorrono. – (*ti do anch'io una mano, forse non indispensabile, per beccare con facilità programma e funzioni. Te ne segnalo un paio. 1) Start/ Pannello di Controllo/ Sistema/ Ripristino . Oppure 2) Risorse del Computer/ Disco C:/ in alto una delle ultime icone è "?" , ci clicko sopra e si apre Guida in Linea/ scelgo l'opzione "Annulla le modifiche apportate con Ripristina Configurazione di Sistema/ mi offre le 2 opzioni: Ripristina o Crea* - NdA)

Chi può aiutarmi ?

A volte nella vita ci sembra di esser soli e che non ci siano vie d'uscita. Per le cose veramente importanti può anche esser vero, soprattutto se non hai la fortuna di credere che esista Qualcuno che in qualche modo una mano te la dà sempre. Qui, col computer, hai solo l'imbarazzo della scelta:

- Un amico smanettone

Ormai i computer sono così diffusi che qualche matto che si diverte a risolvere i problemi, non è difficile da trovare. Basta chiedere, a volte ce l'abbiamo anche in casa o in ufficio. O in qualunque circolo o palestra tu frequenti. (*il Guardiano è schivo e modesto, non vuole dire che come amico lui è disponibile in prima persona, ma è così – NdA*)

- Giornali specializzati

Una mail ad un giornale cartaceo o on-line spesso risolve il problema. Gli fai anche un piacere, c'è addirittura chi ha istituito un premio per il lettore che proponga il quesito più intrigante. Ti faccio qualche esempio:
http://www.pcmag.com/article2/0,2817,2351871,00.asp
Top 20 dei virus presenti in Rete **WinMagazine**
http://punto-informatico.it/canali.aspx?idc=56

- Un valido professionista

Spesso ci buttiamo su offerte che sembrano irresistibili senza pensare al dopo. Nessuno si sognerebbe di comprare un'auto senza accertarsi prima che esista un'adeguata officina di manutenzione. Anzi siamo pure sofistici e la vogliamo comoda, con gente gentile, preparata ecc. Col computer stranamente dimentichiamo tutto questo e per risparmiare qualche pur sacrosanto Euro, dimentichiamo il dopo. Rinunciare ad un centinaio di Euro di risparmio può essere un'ottima forma di assicurazione contro i guai per i successivi tre anni di vita media di un computer. Purchè il tecnico che te lo vende sia effettivamente un tecnico e non un semplice rivenditore. Ma in genere il passaparola aiuta a metterci al sicuro anche su questo punto

- Google

Volutamente ho lasciato per ultimo *Zio* Google, quello che ormai è diventato il compagno fedele di ogni seduta in Internet. Ho fatto una prova lanciando una ricerca con una stringa che riporta l'argomento delle nostre chiacchere. Ecco i risultati, in italiano, inglese, francese e spagnolo – Se conosci cinese e russo puoi sbizzarrirti ben oltre !
Risultati **1** - **10** su circa **232.000** per **minacce informatiche**. (**0,29** secondi) Google Inquiry
Risultati **1** - **10** su circa **33.100.000** per **threats**. (**0,24** secondi)
Risultati **1** - **10** su circa **1.030.000** per **menaces ordinateur**. (**0,26** secondi)
Risultati **1** - **10** su circa **1.400.000** per **amenazas informàtica**. (**0,33** secondi)

A questo punto ho avuto pietà del Guardiano che l'indomani avrebbe dovuto prendere un aereo alle 6 a.m., l'ho ringraziato anche a nome tuo e l'ho accompagnato all'auto. Commosso ha promesso di tornare. Incauto!

Vittorio E.Malvezzi e il Guardiano

TF4 - Software

… Te l'ho già detto, l'animo generoso e aperto del Guardiano lo porta a cercare ogni occasione da condividere di persona con gli amici ...

Stavolta però il nostro incontro è saltato per via di un vulcano il cui nome sembra inventato da Jacovitti, quello del Vittorioso. Roba d'antan, quando i fumetti giapponesi, truculenti e isterici, manco se li immaginavano. Tant'è che il Vittorioso io lo comperavo all'Oratorio. Il Guardiano, che per lavoro è spesso in giro, resta bloccato a Roma. Io, da bieco nordista, in questi tempi raramente mi stacco dall'hinterland milanese. Sia lui che io non abbiamo nulla contro la tecnologia se aiuta a risolvere i problemi, quindi ripieghiamo concordi sui new media. Impavidi, in uno sfavillio di effetti speciali e connessioni digitali, ci siamo messi su una videoconferenza di 1h 05'09". Gratis, grazie a Skype.
Stavolta l'argomento della nostra chiacchierata riguardante i diversi aspetti della sicurezza, ha come punto focale il **SoftWare**. Lo abbiamo diviso in sette punti:

1. **come può aiutare un Software**
2. **Software di lavoro**
3. **Software specifici per le transazioni di borsa**
4. **Software di sicurezza personale**
5. **siamo alle solite, non sono uno smanettone**
6. **chi mi aiuta**

1. come può aiutare un SW

Abbiamo già introdotto il concetto della sicurezza sulla nostra macchina – *attacca il Guardiano* – abbiamo parlato di Anti Virus e forse è il caso di precisare che proprio come ritorniamo a parlarne, è il caso ogni tanto di guardarsi in giro per vedere che cosa succeda nel campo degli Anti Virus. Non parlo solo di un doveroso aggiornamento, senza il quale l'AV è come non averlo, parlo proprio di possibili novità. Siccome la gara Virus contro AV è sempre aperta, così i vari produttori continuano a migliorare le logiche della battaglia e nel farlo spesso si superano l'un l'altro. Val la pena di tenersi aggiornati, se poi il nostro passa dal terzo al quarto posto o viceversa e se tutto sommato noi siamo soddisfatti di come funziona, non è il caso di preoccuparci troppo. Ma se da posizioni di testa dovesse piombare nelle retrovie, gratuito o a pagamento che sia, varrebbe la pena rivedere le nostre scelte. In effetti è il caso di dirlo una volta per tutte. La sicurezza vale qualche decina di Euro ben spesi per l'acquisto di un buon AV, ma il fatto di pagare non è di per sé una garanzia di maggiore efficienza di un concorrente gratuito. Quasi tutti i giornalini cartacei e i siti on line specialistici, di tanto in tanto si dilettano di queste statistiche.
Oggi poi sono incominciati a spuntare gli AV non residenti sul nostro computer, tecnologia "on the cloud" la chiamano: http://www.cloudantivirus.com/en/. Ottimi perché non intasano, sono

sempre aggiornati, difficilmente vengono stoppati da hackers, qualche volta addirittura possiamo farli coesistere col nostro AV residente. Caso eccezionale perché solitamente per gli AV non vale il detto "tanto più, tanto meglio". http://www.surfright.nl/nl/downloads/
Di solito invece di collaborare, i due AV litigano furiosamente identificandosi reciprocamente come possibile minaccia. C'è il sospetto che sia un comportamento anche voluto, per motivi commerciali, ma tant'è: evitiamo di mettere due galli nello stesso pollaio. A meno che uno dei due faccia chicchirichì stando in cima al pollaio, fuori sulle nuvole appunto. Una verifica preventiva ti risolverà il dilemma, magari facendo la prova su una macchina diversa da quella che usi quotidianamente per tradare! La qualità intrinseca va valutata nel lavoro quotidiano. L'importante è trovare un giusto equilibrio tra invadenza (lo chiamano anche 'peso') dell'AV e il risultato che ci riesce a sfornare. Si tratta di un abito quasi su misura, il SW non ci aiuta se invece di proteggerci ci impedisce di lavorare serenamente. L'ideale per l'utente medio è che si faccia dimenticare, che non si faccia sentire e lavori in punta di piedi. Per questo se tutto va liscio è opportuno accertarsi che gli aggiornamenti automatici funzionino e magari ogni tanto lanciare un aggiornamento manuale. Spesso i vantaggi degli AV gratuiti stanno proprio nella loro "leggerezza".

2. Software di lavoro

A volte nello scambiarci i files – *continua Guardiano sorridendomi dalla sua postazione che vedo in un quadratino sul mio video e tuonandomi allegramente nella cuffia* – c'è rischio di trovarci degli "ovetti di Pasqua". Sì, quelli con sorpresina. Anche un professionista a volte riceve materiale che lo lascia perplesso e ricordiamoci sempre di usare la prudenza e il buon senso. Senza scomodare nomi tecnici più o meno ostrogoti, ricordiamoci che non necessariamente chi ci manda una mail dicendo di essere il nostro amico Pippo, sia veramente lui. Se non c'è altro modo di verificare, magari chiamando Pippo (*effettivamente le soluzioni più semplici sono le migliori – NdR*) possiamo caricare il nostro file in una finestrella di un sito che ce lo controllerà gratuitamente, sottoponendolo al vaglio di 30 o 40 AV. Sono impreciso perché sono molto attivi e continuano a migliorare. http://www.virustotal.com/it/ ecco come si presentano: " Virustotal è un servizio che analizza files sospetti e permette la rapida identificazione di virus, worms, trojans, e di tutti i tipi di malware rilevati dai motori antivirus." Come vedi parlano anche in italiano.
Comunque un primo controllo ce lo fa il nostro ISP. Per esempio di solito bloccano di default la spedizione di allegati ".EXE" o ".Dll" quelle estensioni che potrebbero più facilmente far passare Virus. La cautela però ci dice che i codici maligni ormai possono essere accodati praticamente ad ogni file. Non solo a quelli creati con Office o immagini con estensione ".JPG". Quindi attenzione, senza diventare isterici, a tutti i file perché certamente i SW più utilizzati sono i più colpiti, ma nessuno può ritenersi esente a priori. Sospetti possono nascere ad esempio, se qualcosa ti arriva inaspettato o se pesa di più di quel che dovrebbe. Come sempre: logica, attenzione e buon senso. Nel dubbio non fidiamoci ciecamente del nostro AV, inutile fargli fare gli straordinari, ma tentiamo un controllo extra.
Quanto ai casi di sicurezza estrema, siano segreti industriali o indirizzi di affascinanti fanciulle, molto probabilmente l'utente usa già una criptografia ed è qualche gradino più in su del livello a cui stiamo trattando noi ora.

3. Software specifici per le transazioni di borsa

Qui intervengo io per lasciargli tirare il fiato. E gli dico - a proposito di SW dedicato al trading, guarda un po' cosa c'è in rete!
http://www.programtrading.com/DPT/program-trading-software.htm
http://www.stocktradingsoftwarereviews.org/
http://free-trading-software.vista-files.org/
http://www.tradecision.com/product/reviews.htm
http://www.01net.com/telecharger/windows/Bureautique/bourse_et_finance/
http://www.annuat.com/rubrique23.html

http://www.euroset.fr/
http://www.softbull.com/windows/negocios-y-finanzas/bolsa
http://www.abcdatos.com/programas/gestion/bolsayvalores.html

Bello – *ma con disciplina il Guardiano mi riporta sui binari che ci eravamo proposti* – però procediamo con ordine. Ci sono due tipi di SW dedicato:

- La piattaforma offertaci dal nostro fornitore di servizi finanziari
- I SW extra

Tutti hanno come scopo quello di abbassare l'errore umano e soprattutto la componente umana legata all'emotività. Una volta ancora ricordiamoci che un SW troppo invasivo può abbassare le performances della macchina e quindi anche la sua reattività. Nel caso di utilizzo professionale meglio usare una macchina dedicata. Cosa per altro sempre più difficile perché i maggiori Social Network offrono interessanti informazioni e dibattiti finanziari. (*in effetti io sono iscritto per questi argomenti, su LinkedIn e Twitter – NdR*) Proprio per evitare o contrastare i furti di identità, i principali enti finanziari hanno adottato una chiavetta generatrice di codici di sicurezza che fanno la funzione di Pass Word. Hanno incominciato con l'operatività sui conti correnti e poi l'hanno estesa anche al trading.

Già –intervengo io – e mi chiedevo, ingenuo, dove stesse il vantaggio per chi operasse al posto mio sul mio conto titoli. Poi in Rete è trapelata la furbata messa su da un giovanotto:
http://punto-informatico.it/2834571/PI/News/nasdaq-congelati-beni-del-cracker.aspx
http://www.itespresso.it/la-sec-contro-il-pirata-russo-del-trading-online-44112.html
http://www.sec.gov/litigation/complaints/2010/comp21452.pdf
http://m.industry.bnet.com/technology/news-analysis/sec-stocks-boosted-hijacked-accounts/43891/
http://www.f-secure.com/weblog/
Praticamente era un ragazzo pieno di iniziativa. Faceva tutto lui. Si vendeva e si comprava facendosi controparte di conti craccati, ovviamente operando a prezzi come dire ... interessanti, per lui ben inteso!

Il codice generato solitamente ha una validità temporale limitata, - *riprende paziente il Guardiano* - quindi viene coperto il rischio che si creino a priori serie di codici numerici, magari per utilizzarli quando non si disponga della chiavetta. Procedura per altro rischiosa, un po' come scrivere la PW di accesso al computer su un post-it appiccicato sul monitor!
Se hai bisogno di utilizzare in due l'accesso, ti servono due chiavette o almeno devi organizzarti per avere, magari al telefono, una lettura al volo mentre stai caricandola lontano da casa.

4. Software di sicurezza personale

E qui faccio la mia bella figura, segnalando una novità al Guardiano, una suite completa e gratuita http://www.forticlient.com/standard.html . Da anni uso un AV gratuito che, oltre a soddisfare i miei peggiori istinti di Arpagone, è ottimo, leggero e auto-aggiornantesi. Lo integro con qualche altro programma antispyware e un firewall. Questa opportunità scoperta di recente mi apre nuove opportunità. Fra l'altro la configurazione di Sistema richiesta è veramente accettabile: basta qualunque Pentium con RAM minima 128 Mb, quando ormai si litiga sul numero di Gb minimo, e all'hard disk ruba non più di 100 Mb. Gira con OS da Windows 2000 Me fino a Seven. Con mia soddisfazione il Guardiano prende nota.

Interessante, ma vorrei parlarti dei "portachiavi" cioè di quei SW che con una sola PW ti gestiscono in sicurezza tutte le tue PW. La logica che è ben nota a chi utilizzi un Mac. Per chi invece preferisca un PC (*non so perché, ma io che utilizzo un PC, a questo punto mi son fatto piccino – NdR)* deve necessariamente utilizzare un PW Manager, almeno fino a quando qualche nuova release di OS di MS copierà questa funzione. Nessun problema, i più noti sono anche gratuiti. Una ricerca con Google con la stringa "password manager" te li sforna a piacimento. Val la pena ricordare la PW della nostra posta elettronica. Può essere strategica e

rischiosissima se cadesse in mano a qualche male intenzionato. Per come vengono gestite le PW dei siti dove ci registriamo, potrebbe dar via libera ad accessi non autorizzati.

5. siamo alle solite, non sono uno smanettone

Non diamo troppo peso alla tecnologia. Più volte io stesso ho sottolineato che un minimo di conoscenza del mezzo che utilizzo è proprio indispensabile. Ti ricordi l'esempio dell'automobile e della patente? Ma non facciamocene un cruccio, mai confondere il mezzo con il fine.

Le due regole auree sono:
1 il buonsenso
2 quando una cosa è troppo bella per esser vera, molto probabilmente non lo è

E, se proprio non ti basta, ci sono un sacco di posti dove si parla di sicurezza, ad es.:
http://blogs.pcmag.com/securitywatch/

6. chi mi aiuta

Ho trovato recentemente su un sito USA una nuova opzione che forse non è molto tecnologica, ma funziona, eccome. L'hanno battezzata **CAF**. Non riguarda gestioni con l'Agenzia delle Entrate, è un acronimo per '**Call A Friend**' . E noi, nei limiti delle nostre possibilità e capacità, siamo qui per questo.
C'è anche quello che ormai viene chiamato "*il migliore amico dell'uomo, dopo il cane*": manco a dirlo è Google, nelle sue varie versioni. Approfondisci un po' le sue possibilità, lui ti aiuta anche in questo. Per esempio poco usata è la versione "quadrata" accessibile per ora solo dal sito USA. Va ben oltre i soliti Booleani. http://www.google.com/squared

La sicurezza si trova anche nei posti più impensati. Pensa che adesso salta fuori che l'**iPad** avrà anche un trattamento di riguardo in merito alla sicurezza negli aereoporti!!!! http://blogs.pcmag.com/securitywatch/2010/04/ipads_exempt_from_airport_secu.php

Vittorio E. Malvezzi e il Guardiano

TF5 - Reti

... L'appuntamento con il Guardiano oggi è previsto in uno dei posti più romantici di Milano: i Navigli. Altro che Skype sta volta. Roba da giustificare le velenose battutine di mia moglie, la frase più gentile con cui mi saluta mentre esco suona come "i fidanzatini". Fortuna che ci pensano le condizioni meteo a creare un ambiente macho. Un test da duri. Quasi una via di mezzo tra Le Piogge di Ranchipur e La Tempesta Perfetta. Impavidi, tra uno scroscio e un fulmine attacchiamo a parlare di Reti ...

che cosa sono

Devi sapere, *attacca brioso come non mai il Guardiano*, che Francesco Caranti mi ha convertito alle parabole (*vi faccio grazia di quello che ho pensato in quel momento, su come stia peggiorando la grandeur del nostro Guru – NdR*) Quindi in questo modo ti spiegherò la tecnica con cui i documenti vengono spediti nella Grande Rete, con un sistema a pacchetti. Internet è come un immenso puzzle, sai di quelli che facevamo da bambini, dove ogni tessera rappresenta una rete privata. Prima dell'avvento dei protocolli su cui si basa internet come la conosciamo, queste tessere non potevano essere incastrate tra di loro. Con il set di protocolli TCP/IP queste tessere hanno iniziato a poter essere incastrate tra di loro generando la rete pubblica.

Adesso consideriamo la base su cui funziona la veicolazione dell'informazione in Rete. Fa conto di prendere un libro, cioè un malloppo di informazioni, strappi tutti i fogli uno a uno, ci metti su francobollo, mittente , destinatario e lo spedisci. Il francobollo rappresenta le regole di funzionamento. Il guaio sta proprio qui. "In principio" nessuno pensò alle regole di sicurezza, perché tanto era avanzato e innovativo quello che stavano facendo, che in quel momento solo in qualche libro di fantascienza si parlava di sicurezza dei dati. Quindi ecco la semplice verità: tutti i protocolli sono geneticamente insicuri.

Facciamo un altro esempio: se mandiamo delle cartoline agli amici, tutti possono leggere tutto quello che c'è scritto. Nel caso della Rete c'è un'ulteriore aggravante. Non c'è un solo servizio postale, ma migliaia di servizi e milioni di persone che addirittura possono mettere una telecamera nella buca delle lettere. Internet è la Rete delle reti: nel mondo reale la mia cartolina può passare tra le mani di 7 o 8 persone, portinaia compresa se ancora esiste. Ma se per esempio mando una mail diciamo ad un amico in Francia passo attraverso migliaia di reti , le tessere del puzzle appunto, senza neanche sapere quali. A priori il percorso è imprevedibile. Il mio messaggio è come un fulmine che segue le linee di minor resistenza del dielettrico.

come sono vulnerabili

Siccome anche la nostra Lan privata è parte di Internet, fintanto che siamo collegati ne condivide fatalmente i destini. Per tornare al nostro fulmine, o meglio al messaggio che abbiamo spedito, esistono dei routers regionali. Sai quel marchingegno che ti piazzano quando chiedi l'ADSL? Ogni ISP, Internet Service Provider in altre parole il tuo gestore, ha la sua rete che fornisce a te e agli altri clienti. Sperando che non siate in troppi e non vi colleghiate tutti insieme, sennò incominciano i problemi. Bene siccome ogni rete deve interfacciarsi, usa dei collettori. Qui tecnicamente è possibile "sniffare" (*così si esprimono quelli del giro per dire lumare, sbirciare, curiosare, fare gli spioni insomma – NdR*) **tutto il traffico** che in quel momento passa attraverso il collettore ! Ricordati che tutele e sicurezze **lavorano sopra** il protocollo originale.

chi può attaccare chi e che cosa

Le mail girano in chiaro e conseguentemente possono essere lette. Ergo chiunque abbia una certa conoscenza tecnica può accedervi. Esistono e sono disponibili a tutti dei **tools** per rintracciare e leggere qualsiasi cosa. Aspetta non ti disperare … non bisogna mai cedere all'isterismo. Basta sapere e regolarsi di conseguenza. Tu manderesti per cartolina la combinazione della tua cassaforte?

che cosa non fare assolutamente

Per prima cosa decidere e ricordare che cosa sia un dato riservato, la cui conoscenza può crearci una maggiore o minore vulnerabilità. Ad esempio il pericolo più comune è rappresentato dal furto di identità. Ma da cosa è costituita l'identità? E' una serie di informazioni: nome cognome data di nascita etc.., solo che non esiste una serie finita di dati che costituiscono l'identità. In realtà l'identità di una persona è costituita dal quel particolare set di informazioni che ci vengono chiesti per fare un qualcosa.
Come ad esempio chiedere un prestito per acquistare l'automobile: Nome cognome codice fiscale e busta paga, questultima costituita da un pezzo di carta su cui c'è scritto che guadagniamo un pacco di denaro.

Tu Vittorio per esempio che mandi la tua carta da lettere con tanto di codice fiscale, già comunichi qualcosa che teoricamente potrebbe essere molto pericoloso.

Si, ribatto io, ma a volte è doveroso farlo e comunque esistono anche programmini disponibili a tutti che permettono di ricostruirlo. Certo che così io gli spiano la strada.

Comunque, *riprende lui*, ci sono pronte delle contromisure. Centrale Rischi ha inaugurato un servizio, a pagamento ma molto economico. Si chiama **Identikit** e ti avvisa quando qualcuno chiede controlli per approvare acquisti con il tuo nome. Un po' come la logica degli SMS che ti arrivano quando toccano il tuo Conto Corrente. Questo è un servizio utilissimo, fornito ormai dalla maggior parte degli istituti bancari, abbastanza conosciuto, ma che varrebbe la pena di non trascurare.

Piccoli accorgimenti possono aiutare. Fai attenzione quando vai sui Social Networks. Per esempio se vuoi mettere la tua data di nascita, potresti lasciala incompleta. Se metti solo giorno e mese ti fanno gli auguri, ma nessuno può ricostruire la data completa. Sempre che da qualche altra parte non ci sia già. E' una lotta! per esempio se per qualche ragione un giornale ha parlato di te, tieni presente che spesso per identificare una persona oltre al nome e cognome mettono l'età. Male, perché oltre a far cosa non troppo gradita a chi i vent'anni li ha passati da un po', aggiungono un pezzetto di dato sensibile.

Se mandi qualche informazione che può renderti vulnerabile, almeno cerca di spezzarla in due messaggi inviati con due modi diversi. Magari uno per SMS e l'altro per email. Crearsi sempre una seconda linea di difesa, insomma.

Decidere poi quale sia il limite di perdita sopportabile. Se giro in bici in una grande città, ci sono forti probabilità che prima o poi me la rubino. Posso sopportare questo furto? Sennò meglio girare in tram o Metro. Stessa logica in Rete. Non pensare poi che gli hackers siano sempre e solo lì per danneggiarti. Certi tipi di attacchi hanno indirettamente contribuito a migliorare la sicurezza.

Ci metto anche del mio, continuando diligentemente a fare i compiti. In questi siti ci sono suggerimenti e linee guida base. Per giovani e adulti.
http://kidshealth.org/teen/safety/safebasics/internet_safety.html
http://www.wikihow.com/Be-Safe-on-the-Internet *questo ci dà veramente alcuni dati che vale la pena ricordare: "Here are a few ways to stay safe during your online activities". Sono in inglese, ma si tratta di regolette estremamente chiare. Riepilogano alcuni comportamenti che*

dovrebbero essere alla base di ogni condotta dettata da buon senso e prudenza. Non sto a ripeterteli, ma ogni tanto vale la pena di andare a dargli una scorsa.

che cosa fare, tanto per cominciare

On line trovi anche qui una serie di suggerimenti pratici. Quelli che io chiamo usare il buon senso.

Faccio il compitino e vado cercare in giro sulla Rete:
http://www.pier55.com/Internet/safe-internet-surfing.shtml *ci regala le* **Basic Rules of Safe Internet Surfing .** *Si potrebbero riassumere in quello che il Guardiano chiama "Regole di Buon Senso" , ma tanto per esagerare, richiamiamole qui.*

- Usa i programmi di Protezione (firewall, AV, antispyware , ecc)
- Tieni aggiornati sistema e difese
- Non credere ciecamente a nessuno
- Leggi anche quello scritto in caratteri piccoli !
- Pensaci su due volte prima di clickare

Poi ci sono le cose serie, *riprende il Guardiano*, parlo della Crittografia e ti spiego la tecnica della doppia chiave con un'altra parabola. (*il Guru sta volta ha creato un Mostro! – NdR*) Fa conto che io metta un messaggio segretissimo in una scatola, se preferisci un'atmosfera più intensa chiamala cassaforte o forziere. Doverosamente applico un lucchettaccio e te la spedisco. Tu la ricevi e senza tentare di aprire, cosa quasi impossibile, ci applichi anche tu un altro lucchettaccio a tua garanzia e me la rimandi. Così quando mi ritorna io tolgo il mio catenaccio e il forziere resta ancora in sicurezza, ma sta volta **solo grazie al tuo catenaccio**. Quindi quando ti ritorna per la seconda volta, sempre protettissimo, c'è solo il tuo lucchetto che puoi aprire e finalmente leggere sto dannato messaggio ballerino. (*devo ammettere obtorto collo, che sta storia della parabola, funziona! almeno con me – NdR*)

chi ci aiuta

Esistono delle organizzazioni pubbliche in Italia e nel mondo preposte proprio alla difesa della sicurezza. Prova ad esempio a digitare **Nist** l'ente di standardizzazione che ha abbracciato la filosofia del "security by design" http://en.wikipedia.org/wiki/Security_by_design .

Eseguo da bravo allievo: http://www.nist.gov/itl/csd/itl_031009.cfm *hanno un preciso compito e ti suggeriscono le guidelines per una safer Net Surfing. Peccato che ti buttino su una pagina inesistente e poi gli stolti mi hanno anche tampinato per chiedermi un parere dicendomi che ero stato selezionato per l'intervista. O sono stati sfigati o imprudenti, comunque ho risposto. Adeguatamente.*
*In compenso buttando dentro a Google la stringa "**Safer Net Surfing***
Buttando dentro a Google la stringa <safer net surfing> ottieni Circa 3.640.000 risultati (0,26 secondi)
*Se scrivi "**navigare Internet in sicurezza**" ottieni Circa 496.000 risultati (0,21 secondi) sono meno, ma forse è più facile, infatti uno dei primi ritorni è:*
http://news.wintricks.it/web/sicurezza/27851/decalogo-per-navigare-sicuri-in-internet/

E poi ci siamo qua noi, no? *aggiunge sogghignando il Guardiano …*

Vittorio E. Malvezzi e il Guardiano