SELEZIONE MIRATA

CIRCOLARI
ATTIVITA'
NOTIZIE
ORARIO LEZIONI
MODULISTICA
DIDATTICA
COMPUTER-Guide-Video
- Tutte le Categorie
- Manutenzione PC
- **Utilità & Sicurezza**
- Software Win Gratuito
- Ubuntu Videoguide
- Software Libero e Guide
- Software Libero Articoli
- Le Vostre Risorse

FAQs-Domande Frequenti
BLOG
WEB-LINK
CONTATTIAMOCI
MAPPA del SITO
MEDIA-Curiosità-Svago
LA TUA POSTA
PIAZZA GRANDE
I VISITATORI CI SCRIVONO
VECCHIO SITO MAJORANA

DIZIONARI-ENCICLOPEDIE
LEGISLAZIONE-NORMATIVA
Educazione alla Cittadinanza
CORSI Formazione Docenti

FEEDS - Tenetevi Aggiornati

feeds RSS per un aggiornamento in tempo reale. Ecco la guida ai feeds

- *Circolari Istituto "E.Majorana"*
- *Attività scolastiche ed extra*
- *Guide Software per Linux*
- *Guide "Free-Soft" Windows*
- *Tutto su: Informatica del sito*
- *Tutte le "Categorie" del sito*

Software Libero - The Best

ALTRE NOSTRE PAGINE CONSIGLIATE

Google Traduttore
Seleziona lingua
Gadgets powered by Google

Software Libero Bilancio	*SicEnea-*
Ridiamo di Noi	*SportelloAscolto*
I Visitatori Scrivono	*Conferenze e Viaggi*
	Classi-Giochi-Curiosità

SITO OTTIMIZZATO PER RISOLUZIONE 1024x768

SITI UFFICIALI che pubblicano le nostre VIDEOGUIDE

Click sulle immagini per gli articoli

HOME ▪ COMPUTER-Guide-Video ▪ Utilità & Sicurezza ▪ Sicurezza: i dieci comandamenti

Sicurezza: i dieci comandamenti

PDF PRINT EMAIL

Valutazione utente: / 32
Scarso Ottimo Valuta questo articolo

Scritto da Prof. Ing. Antonio Cantaro: amministratore

martedì 12 febbraio 2008

Questo articolo contiene una Video Guida del Prof. Ing. Antonio Cantaro

Fase-1 – I dieci comandamenti della sicurezza PC

Premessa

Se il computer si spegne senza chiederlo, se strane finestre con testo incomprensibile e tutti i tipi di avvertenze appaiono senza che tu lo chieda, se delle email vengono inviate a tutti i tuoi contatti a tua insaputa, allora il tuo computer ha probabilmente contratto un virus o qualcosa di simile che chiameremo genericamente malware (ve ne sono di tantissimi tipi ed hanno caratteristiche diverse). La causa principale è addebitabile al fatto che usi Windows. Linux difficilmente contrae dei virus, tanto che non necessita neppure di antivirus.

Con l'espandersi dell'utilizzazione di internet questi pericoli sono aumentati in maniera esponenziale. Mentre prima il virus lo si prendeva con i dischetti (floppy) che magari ci si scambiava tra amici, oggi le porte d'ingresso sono aumentate. Basti pensare a CD o DVD di dubbia provenienza (soprattutto per i contenuti), alle penne (pen drive) che saltano da un computer ad un altro (basta che uno sia infettato ed ecco che la penna diventa un mezzo di diffusione estremamente efficace). Chi scrive opera in ambito scolastico ed in sala professori è sistemato un computer col quale molti colleghi si scambiano dati, informazioni, file e risorse. Tante, quindi, le ***"pen drive"*** che circolano. Morale della favola: l'antivirus è sempre in continuo allarme ed avvolte non risolve il problema e quindi si ha una nuova infezione generalizzata e difficile da estirpare. Ma come già detto, oggi, il mezzo di maggiore diffusione di queste piaghe informatiche, è certamente internet.

Il software è sempre più sofisticato e quindi più complesso e delicato, questo significa pure che è più vulnerabile, in quanto, nella sua complessità, lascia delle porte che, i malintenzionati più esperti, riescono a scovare ed utilizzare per entrare nel nostro PC. Avrete sentito parlare di **patch** (letteralmente "pezza"), non sono altro che degli aggiustamenti ai programmi, miranti a chiudere qualche falla di sicurezza delle applicazioni che man mano viene scoperta. La Microsoft (e non solo) ci ha abituato a questo genere di rappezzo per il tramite dei frequenti aggiornamenti. Ma chi produce e diffonde questi virus? Sicuramente malintenzionati, burloni, esaltati, e gente che magari non ha altro da fare. Alcune voci, nel web, insinuano che anche qualche produttore di antivirus, diffonda questo genere di cose, magari per tenere caldo il mercato. Sicuramente si tratta di gente esperta in informatica. Pensate quanto bello sarebbe non avere la preoccupazione della sicurezza. Peraltro tutti i nostri sistemi di sicurezza rallentano notevolmente il computer. Purtroppo la realtà è questa e bisogna difendersi.

Cosa sono i virus ed il malware in genere

Un virus è un programma molto simile a quelli che utilizziamo quotidianamente, spesso piccolo in dimensioni ma scattante. La sua caratteristica principale è quella di essere progettato per causare danni al personal computer su cui viene eseguito ed in particolare ai dati in esso memorizzati. Se, da un lato, esistono virus innocui che si limitano a presentarsi con strani effetti grafici, gran parte dei virus, una volta insediatisi all'interno del sistema, è capace di eliminare file, rinominare a caso documenti ed immagini, sovrascrivere file importanti. Riescono anche ad inviare, per via posta elettronica ed all'insaputa del proprietario del computer "vittima", testi, immagini e quant'altro, memorizzato sul proprio disco fisso, a colleghi, amici, conoscenti. Certi virus, non appena avviati, si presentano in modo appariscente visualizzando messaggi sullo schermo o strani effetti grafici; la maggior parte, invece, "lavora" in modo subdolo e senza che l'utente se ne accorga.

Accanto ai virus "tradizionali" troviamo, poi, il cosiddetto malware, che comprende un enorme numero di sottocategorie. Tralasciando la loro elencazione diremo subito che si tratta di particolari programmi "maligni" che, se eseguiti, rendono il personal computer preda facile da parte di attacchi dall'esterno, generalmente perpetrati via Internet, mentre si è collegati. Quasi tutti cercano di accedere ai dati memorizzati sul disco fisso per carpire informazioni e notizie di ogni genere (dagli indirizzi di posta elettronica, alle password, ai documenti importanti e così via dicendo). Addirittura vi sono dei malware (keylogger) che registrano le sequenze dei tasti che digitiamo sulla tastiera, per poi trasmetterli a chi ci ha infettato. Si pensi alla password dei servizi bancari on-line ed al pericolo per i nostri soldi. Certamente la nostra sicurezza ha valore, almeno economicamente, meno importante rispetto ad una azienda o industria (segreti industriali) ma questo non vuol dire che non dobbiamo preoccuparcene.

I dieci comandamenti

Ormai siamo al cane che si morde la coda. Ogni giorno nuovi virus, nuove pezze, nuovi antivirus, nuovi virus, nuove pezze …. Però se ci abituiamo a piccole ma importanti abitudini, da soli possiamo fronteggiare una grossa parte dei pericoli. Ecco alcuni semplici ma efficaci consigli.

1 – Non frequentare siti pericolosi. Sono soprattutto i siti che offrono "crack" (per sproteggere i programmi a pagamento) o risorse pirata (programmi, musica, film, ecc…) i più pericolosi, anche se avvolte siti apparentemente innocui ci riservano brutte sorprese. Nessuno ***o quasi*** lavora per il semplice piacere di regalarti qualcosa (chi scrive fa parte di quei pochi che lavorano disinteressatamente e senza scopi oscuri, per la sola soddisfazione di porgere ad altri le proprie conoscenze). Quindi state certi che entrando in siffatti siti vi beccherete immediatamente o al massimo dopo pochi minuti il ***"virus"***.

2 – Diffida dei regali altrui. Non fidatevi di chi vi regala programmi, risorse grafiche (le sorprese le possiamo trovare anche dentro una semplice ed apparentemente innocua immagine grafica), giochi od altro, spesso contengono dei "troian" (cavallo di Troia), ossia dietro un bel regalo allettante, ecco la serpe nascosta e pronta a colpire. Prima di accettare, scaricare ed istallare siffatte risorse, siate certi della serietà di chi ve le offre. Esistono certamente persone ed aziende serie da cui accettare regali ma attenzione alla marea di gentaglia che con la scusa del regalo vuole solo fare i propri sporchi interessi.

3 – Attento allo scambio dati. Capisco che è impossibile non utilizzare la "pen drive", magari l'amico o il collega vuole darci qualcosa o siamo noi a volergli dare quel documento, quella foto o quel programma particolare. Facciamolo pure, però ricordatevi, prima di mettere la penna nel vostro computer, di controllare che l'antivirus (se lo avete anche l'antispyware, ecc…) sia ben funzionante e soprattutto ben aggiornato. Così facendo i rischi diminuiscono e di molto. Stesso discorso, ovviamente, vale per CD, DVD , floppy ed ogni altro dispositivo di memoria di massa.

4 – Occhio alla posta elettronica. Non aprite mai allegati che vi giungono da persone sconosciute, potrebbero riservarvi brutte sorprese. Purtroppo può capitare che proprio i malintenzionati si siano impadroniti della rubrica di un nostro conoscente ed abbiano utilizzato gli indirizzi ivi contenuti per le loro scorribande. Quindi se pure conosciamo il mittente, in questo caso, potremmo avere l'amara sorpresa. Sarebbe bene contattare l'amico o il conoscente ed accertarci se proprio lui ci ha inviato l'e-mail col relativo allegato. Comunque non crediate di essere al sicuro non aprendo gli allegati della posta elettronica: gran parte dei virus sanno "auto-eseguirsi" anche senza il classico doppio clic sull'allegato, proprio grazie alle falle esistenti nel sistema. L'invito a riflettere più e più volte, prima dell'apertura di un allegato, è sempre valido. Un antivirus aggiornato, che controlla attivamente la posta, aiuta notevolmente.

5 – Aggiorna il sistema. Tenere sempre aggiornati i programmi utilizzati ad iniziare dal sistema operativo, quindi browser (programma per navigare tipo internet explorer, firefox, ecc…), i player, java, ecc…

6 – Aggiorna l'Antivirus. Aggiornare frequentemente l'antivirus, gli antispyware ed i programmi di protezione e difesa in genere. Lo scrivente lo fa ogni giorno. Basta fare l'abitudine. Aggiornando spesso serve solo poco tempo. Aggiornamenti distanziati richiedono tempi più lunghi.

7 – Usa un "firewall". Firewall significa parete o muro di fuoco. In pratica è una barriera tra il nostro computer e la rete. Esso controlla il traffico sia in entrata che in uscita. Se installato e ben configurato un firewall

protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente. Anche Windows XP ha un firewall di "serie" (non sarà dei migliori, comunque è già una buona cosa).

8 – Fai il Backup dei dati. Si tratta di fare la copia di sicurezza dei propri dati e del lavoro svolto. Quanta gente ho visto piangere amaramente dopo avere perso settimane, mesi e qualche volta pure anni di lavoro. Tutto in un solo attimo. Fino a quando non ci capita personalmente non ci rendiamo conto dell'importanza del bakup. A me capitò molti anni addietro, da allora e dopo la dura lezione, non è più capitato, grazie alle precauzioni che ormai uso abitudinariamente. Sarebbe buona norma effettuare la copia di sicurezza dei dati dopo una giornata di lavoro. Ancora meglio (costa meno fatica ed è più semplice per gran parte di noi che non siamo una banca o una grossa azienda) fare la doppia copia immediata. Mi spiego meglio con un esempio. Magari abbiamo finito di scrivere un documento oltre che salvarlo normalmente, salviamolo pure in un altro hard disk (almeno in un'latra partizione), in una pen drive, in un CD o DVD riscrivibile, insomma dove vogliamo, purché non dove risiede il sistema operativo. Per fare tanto basta solo qualche click in più, pochi secondi. Abituiamoci, al momento opportuno non serviranno i santi in paradiso, ci saremo salvati da soli. Dopo avere fatto questo, ogni tanto riorganizziamo i dati e creiamoci gli archivi di riserva quali CD, DVD, hard disk esterno, ecc.. Per dati particolarmente importanti sarebbe bene avere almeno un doppio archivio quale riserva estrema.

9 – Partiziona bene l'HD. Cercate di avere almeno due partizioni nell'hard disk. Una contenente il sistema operativo ed i programmi (applicazioni), l'altra contenente i dati, la documentazione, i media ed altro. Anche un secondo hard disk non sarebbe male. Ricordatevi che le precauzioni non sono mai troppe. Vi rammento che molte aziende spendono milioni di euro per la sicurezza informatica di ogni genere.

10 – Crea l'immagine di sistema. Effettuare l'immagine di sistema è una cosa estremamente utile. In pratica dopo avere istallato il sistema operativo, ed il software applicativo (tutti i programmi da noi utilizzati), previa una bella ordinata e messa a punto di tutto, si procede a creare la copia dell'intera partizione, con dei programmi specifici (vi sono ottimi programmi commerciali ed anche gratuiti). In caso di bisogno (virus, sistema lento, danneggiato od altro) basterà fare il "restore" per avere il computer così com'era quando avevamo fatto l'immagine. Guardate che non parlo del "ripristino configurazione del sistema" di windows che è una cosa molto limitata e che non sempre funziona o riesce. Sto parlando di riottenere in pochi minuti tutto e nella stessa identica maniera di come l'avevo conservato in precedenza. Istallando e disistallando molti programmi, per studio o prove o facendo sperimentazione, nel volgere di qualche settimana (come a me capita) bisogna riformattare tutto, reistallare tutti i programmi e fare i settaggi di nostro gusto. In pratica un giorno di lavoro. Lo stesso lavoro, con l'immagine di sistema, si può fare in un quarto d'ora e senza fatica. Io ho una ventina di immagini. Ogni volta che ritengo di effettuare importanti aggiornamenti, carico l'ultima immagine che ho realizzato (quindi parto sempre da un sistema pulito, perfettamente funzionante ed agile). Aggiorno il sistema e le applicazioni che mi interessano, effettup la messa a punto e rifaccio una nuova immagine. Sono di nuovo pronto a sbizzarrirmi e fare quello che voglio (pure navigare in siti poco sicuri). Ho trattato con molta attenzione quest'argomento e, per un ottimo programma gratuito che trovate insieme con le videoguide, in italiano, vi rimando alla pagina:

Riformattare no grazie-Immagine sistema

Tutti i consigli dati sono sicuramente utili, ma innanzi a tutto dovremo mettere la formazione della nostra mentalità. Bisogna abituarsi alle cose giuste in maniera che divengano quotidianità e normalità. Certo potrei dare molti altri consigli in aggiunta ai precedenti, ma il troppo storpia. Da soli impereremo, dopo l'acquisizione delle buone abitudini, a perfezionare i nostri comportamenti. Se solo riuscissimo a fare quanto finquì esposto, avremmo sicuramente raggiunto un ottimo livello. La certezza della sicurezza totale è solo una favola, ci sarà sempre qualcuno che ne inventa una nuova pur di fare guai agli altri.

Concludo dicendo che, io, non amo gli aggiornamenti automatici. Preferisco effettuali manualmente perché non voglio che gli altri lavorino, a mia insaputa, sulla mia macchina. Però, gli aggiornamenti, li faccio e spesso! Ritengo giusto che ognuno si regoli secondo i propri criteri, pertanto reputo opportuno indicare, almeno, come settare Wndows XP, dal punto di vista dei sistemi di sicurezza. Più di tante parole vale un video d'esempio, ecco la video guida:

Centro sicurezza PC ⬅ **Video guida**

Ultimo aggiornamento (domenica 05 luglio 2009)

< Prec. **Pros. >**

[Indietro]

IISS "E. Majorana - Gela (CL)
Geometri - Servizi Sociali - Geometri Serale - Istituto d'Arte
Tel. 0933-93.04.64 - email:
amministratore@istitutomajorana.it