

Dieci semplici regole di prudenza - Guida scaricata da www.manuali.net

Regola n. 1: la prima e semplice regola, banale se si vuole, è quella di tenere SEMPRE aggiornato il proprio antivirus. Ci sono antivirus più o meno efficaci e ognuno può avere le proprie preferenze e le proprie comodità nell'uso di un programma specifico. L'unica cosa essenziale però rimane quella di AGGIORNARE periodicamente, a scadenze fisse, il proprio antivirus. Vengono individuati sempre nuovi virus ed un antivirus non aggiornato non serve a nulla.

Regola n. 2: quando si riceve una e-mail, la prima cosa da fare è controllare da chi proviene. Se proviene da una persona conosciuta, si può procedere alla lettura del testo della lettera. Se proviene da una persona che non si conosce, bisogna cominciare ad avere i primi dubbi e a SOSPETTARE dell'e-mail. A maggior ragione i sospetti si devono intensificare se tale e-mail ha degli allegati. I virus possono essere presi anche leggendo semplicemente una e-mail. Ma tali tipi di virus sono abbastanza rari. Le e-mail che contengono virus sono nella stragrande maggioranza dei casi contenuti negli allegati e dunque BASTA NON APRIRE l'allegato e CANCELLARE l'e-mail. Si gioca, in questi casi, sull'elemento psicologico della curiosità, ma davvero si vuol rischiare di prendere un virus solo per vedere l'allegato di una persona che neppure si conosce?

Regola n. 3: purtroppo le e-mail che contengono virus possono avere come mittente una persona che a noi è nota e che è presente tra i nostri contatti e nella nostra rubrica. Questo avviene perché molti virus una volta infettato un computer, scandagliano la memoria e la rubrica e si auto-inviano a tutti gli indirizzi presenti sul computer. Cosa fare in questi casi? Come riconoscere il possibile virus? Verifichiamo l'oggetto del messaggio. Moltissimi virus sono in inglese. Quindi se l'oggetto è in inglese, è sempre meglio, per prudenza, avere un piccolo sospetto sulla vera natura di tale e-mail. A questo punto sappiamo che l'e-mail proviene da una persona che conosciamo, che è in inglese e che ha uno o più allegati. Come agire? Verifichiamo il testo. Il testo risulta essere interamente in inglese, e non solamente alcune frasi o parole: può anche capitare che per gioco o per necessità si debba ricorrere all'uso di un'altra lingua. Oggettivamente quante persone conosciamo che ci scrivono un'intera e-mail in inglese? Oppure può capitare che noi conosciamo delle persone che ci scrivono in inglese, perché non sono italiane, ma l'e-mail, in questo caso, non l'abbiamo ricevuta da queste persone. La qual cosa dovrebbe metterci per lo meno in guardia. Anche nel caso in cui, l'e-mail fosse stata scritta in italiano e provenga da amici che parlano correttamente l'italiano o comunque che la lettera fosse stata scritta in inglese e provenga da amici che non parlano l'italiano, bisogna sospettare della mail in questione nel caso in cui le frasi in essa contenute siano prive di connessione logica o risultino essere del tutto insensate e sconclusionate. Ci sono virus infatti che scelgono a caso dai nostri documenti pezzi di frasi e le assemblano. Ma ovviamente non avranno un senso lineare e logico. Cosa fare? Se questa e-mail ci pare essere estremamente sospetta, chiediamo conferma al nostro amico/a se effettivamente ci ha spedito tale e-mail. Non ci costa nulla chiedere: i virus si inviano all'insaputa della persona dalla quale essa proviene e se dunque quest'ultima non ne sa nulla, meglio provvedere a CANCELLARLA. Se invece c'è la conferma che è stata volutamente spedita, possiamo aprirla.

Regola n. 4: MAI scaricare dialers di connessione da siti che ci propongono di farlo. Mai, mai e poi mai farlo perché sono delle "truffe" belle e buone. Non penso valga la pena di pagare milioni in bollette telefoniche per avere una suoneria o uno sfondo.

Regola n. 5: MAI scaricare da internet un qualche cosa che non si sa bene cosa sia. E soprattutto MAI installarlo. Se non si è sicuri di cosa sia ed a cosa serva un determinato programma, chiedere ad amici, ai forum, a persone un po' più esperte. Se sono programmi validi, saranno di certo conosciuti. A parte il pericolo di virus, dialers e quant'altro, vi è sempre il rischio di possibili

incompatibilità con altri programmi e disfunzionamenti di windows. Molto spesso risolvibili con una disinstallazione del programma. Ma altrettanto spesso, possono essere programmi che contengono sotto-programmi spioni, come ad esempio il GAIN nel Divx. Disinstallando il Divx, non si elimina questo spy. E il nostro computer continuerà a rilasciare informazioni, e non si sa bene quali e di che genere, su di noi a non si sa bene chi! Inquietante ...

Regola n. 6: MAI e poi MAI, e lo sottolineo una terza volta, MAI, lasciare il proprio indirizzo di posta elettronica a persone che non si conoscono, lasciarlo sui siti, lasciarlo sui guestbook dei siti, metterlo nelle registrazioni per accedere a siti o al download di programmi. Il vero problema è che molti siti o programmi (come quando si procede alla registrazione di un programma) ti richiedono esplicitamente l'indirizzo di posta elettronica per effettuare una registrazione. Non penso però valga la pena di ritrovarsi la posta elettronica invasa di spam e di virus (perché attraverso lo spam possono arrivare anche virus) solo per registrarsi ad un sito, lasciare un messaggio su di un sito in un guestbook o registrare un programma. Cosa fare in questi casi? Apriamo un indirizzo di posta elettronica (account) SECONDARIO e utilizziamolo esclusivamente per questo. Separiamo il nostro indirizzo primario, cioè quello che è utilizzato abitualmente solo per amici o altro, dal nostro indirizzo secondario, utilizzato per questi scopi. Vedrete che in breve tempo, uno sarà sempre libero da spam, l'altro sarà pieno. Ci sono molti siti che offrono la possibilità di aprire mail-box gratuite, come www.email.it, www.katamail.com, www.hotmail.com, www.yahoo.it, www.lycos.it e via dicendo. Se non si sa come procedere per aprirne uno, consultate il forum sulla posta elettronica o chiedete aiuto.

Regola n. 7: le funzioni Cc e Ccn (Bcc in inglese) dei programmi di posta elettronica e in genere presente in tutte le mail-box. Avete mai notato che quando scrivete un messaggio di posta elettronica oltre che a essere presente il campo "A" ("To" in inglese) quale destinatario dell'e-mail ci sono anche i campi sopra menzionati? Bene! La funzione Cc (che significa Copia Carbone) è una funzione che permette di mandare questa stessa e-mail a più persone, inserendo semplicemente, ulteriori indirizzi di posta elettronica. In questo primo caso, tutti i destinatari dell'e-mail, saranno a conoscenza degli indirizzi di posta elettronica di tutte le persone a cui voi avete mandato l'e-mail. Vi sarà capitato anche a voi di ricevere una e-mail a catena ricolma di indirizzi di posta elettronica. Questa ne è la causa. La funzione Ccn (che significa "copia carbone nascosta" - "BCC" in inglese) permette di mandare una e-mail a più persone, ma senza che quest'ultime siano in grado di sapere gli indirizzi di posta a cui voi avete mandato l'e-mail. Io consiglio di usare sempre la funzione Ccn ("Bcc") a meno che non vogliate esplicitamente far sì che i destinatari siano a conoscenza del fatto che avete mandato una e-mail ad altre persone (come quando, in ambito lavorativo, si manda una copia per conoscenza ad altre persone). So perfettamente che è sempre più comodo fare "inoltre" quando si riceve una e-mail a catena, ma in tal modo le e-mail si riempiono di indirizzi di posta elettronica e se tali e-mail finiscono in mani sbagliate, avremo come risultato di avere la casella di posta elettronica invasa da spam, cioè da posta indesiderata, e da virus (perché capita non di rado che tra lo spam, non vi sia solo la noiosissima posta pornografica, ma anche virus).

Regola n. 8: installare ed avere non solo un buon antivirus aggiornato, ma anche un firewall (un programma che inibisce l'accesso e la connessione al e dal proprio computer se non dietro vostra autorizzazione), un antispy (tra i più noti e consigliati: Ad-aware E Spybot), e un antitrojans. Gli spy sono programmi spioni che si infiltrano nel computer e rilasciano informazioni su di noi a terzi. I trojan-horse (cavalli di troia) sono programmi che si insinuano nel pc e permettono ad un terzo di assumere il controllo del nostro pc, sottraendo password e codici o facendo partire, tramite il computer, attacchi informatici. Un buon antivirus dovrebbe proteggere il computer anche dai trojans, ovviamente. Ma vi sono moltissimi tipi di antivirus, più o meno efficaci e con cui, a seconda dei gusti e delle comodità, ci si trova comodi. Un antitrojans, offre comunque uno strumento in più di difesa ed è giusto conoscerne l'esistenza.

Se non si sa quali e dove trovarli, in questo link ne sono presenti moltissimi gratuiti:

<http://www.manuali.net/forum/showth...;threadid=18474>

Si possono trovare anche consigli su come comportarsi e su come agire. L'utilizzo di tali programmi, non potranno garantire una sicurezza del 100% al vostro computer e ai vostri dati. Ma almeno offrono una diminuzione di probabilità di passare dei "guai".

Regola n. 9: tenere sempre aggiornato il proprio pc con le patch di sicurezza rilasciate dalla Microsoft. A questo riguardo consiglio sempre di provvedere all'aggiornamento del proprio pc solo ed esclusivamente dal sito della Microsoft (da internet explorer andare su STRUMENTI e poi su WINDOWS UPDATE e vi collegherete subito). Non seguite altre strade, se non è necessario, ma soprattutto meglio non installare subito le patch rilasciate. Capita sovente che tali patch provochino dei rallentamenti o dei problemi al computer. Meglio dunque lasciar passare un periodo di rodaggio. Molte patch comunque, anche se non tutte, possono essere disinstallate. Prendersi nota del numero e del nome della patch nel caso si venga a sapere che essa provoca disguidi (o se in seguito all'installazione registriamo delle anomalie nel nostro computer che prima non c'erano): in tal modo possiamo procedere alla disinstallazione e attendere magari che escano delle patch cumulative (c.d. service pack).

Regola n. 10: nel caso in cui capita di prendersi un virus, la prima cosa da fare è MANTENERE LA CALMA. Alla fine si tratta sempre di un problema di carattere software ed è dunque risolvibile. E' più noioso quando ad esempio si rompe una componente hardware (la ram, il masterizzatore, la ventola, la scheda madre, etc) e bisogna attendere per portare il pc da un tecnico che sia in grado di riparare il computer e sostituire il pezzo. E guarda caso, capita sempre di sabato, domenica o sotto le feste. Se si prende un virus, mal che vada, nell'ipotesi più negativa, se non si riesce a ripulire il pc con un kit o un tools di rimozione, si può sempre formattare il pc (anche se in vero ci sono virus che non risiedono sull'harddisk e non possono essere rimossi con una formattazione, ma sono rarissimi). Per questo è IMPORTANTISSIMO farsi una copia di tutti i nostri dati (dai documenti alle email) e masterizzarli su cd o comunque metterli anche su un harddisk secondario. La formattazione è una procedura che consiste nel cancellare completamente tutto il contenuto del computer e la successiva reinstallazione di tutti i programmi per farlo tornare come quando lo si è comperato: esistono dei programmi che agevolano tali procedure come DriveImage che danno la possibilità di creare un'immagine del proprio harddisk in modo da diminuire i tempi di reinstallazione. La formattazione dura poco, il lavoro vero consiste nel reinstallare tutti i nostri programmi e ci vuole tempo. E da notare infine che tutti i nuovi pc, vengono forniti con dei cd di RECOVERY o di RESTORE .. e servono appunto a far tornare il pc con le impostazioni e i programmi di quando lo si è comperato. La formattazione comunque è l'ultima risorsa. La prima cosa da fare è identificare il virus e l'antivirus dovrebbe darti delle informazioni al riguardo. La seconda è verificare sui motori di ricerca (www.google.com) il nome del virus e se sui siti delle case produttrici di antivirus ci sono dei tools specifici di rimozione. La terza, per sicurezza, è di provvedere alla scansione del proprio pc con antivirus on-line. Per vedere quali sono i siti che offrono tali servizi, consultare il link che ho citato alla regola n. 8. Infine chiedere aiuto al nostro forum sui virus.