Lavorare in Sicurezza

Abbiamo elaborato un riassunto dei principali consigli che vi serviranno per lavorare in sicurezza. Una vera e propria **guida alla sopravvivenza** che vi aiuterà a mettervi al riparo dai virus e dagli attacchi.
Ognuno dei seguenti suggerimenti vi permetterà di lavorare in sicurezza

1. **Non aprite mai**... un file arrivato (**tramite posta elettronica**) e non richiesto da voi, indipendentemente da chi sia il mittente.

2. **Non aprite** alcun messaggio o file arrivato attraverso la posta elettronica da parte **di fonti sconosciute** o **poco conosciute**. Nel caso in cui esso provenga da persona conosciuta bisogna ugualmente usare le precauzioni corrispondenti in merito ai file ricevuti. ***Accordatevi*** con il mittente per l'invio di file (la maggior parte dei virus attuali si possono ricevere da mittenti conosciuti che inconsapevolmente inviano i virus insieme ai loro messaggi).

3. **Non eseguite direttamente** (doppio clic) i file ricevuti ma conservateli prima in una cartella temporanea per effettuare un controllo su di essa con almeno due o tre antivirus aggiornati prima di essere eseguiti (.EXE) o aperti (.DOC, .RTF, ecc.). Se avete dubbi sulla bontà del file semplicemente bisogna cancellare il messaggio (ed i files ad esso accodati).

4. I files eseguibili o che possano causare modifiche semplicemente aprendoli (esempio: EXE, COM, BAT, REG, DLL, VBS, SCR, LNK, ecc..) o che contengano **macro** (DOC, RTF, XLS, ecc..) non vanno accettati via e-mail. I files RTF (Rich Text Format), non possono contenere macro, ma si possono rinominare come file .DOC o come file .RTF ed in questo caso Word li aprirà senza avvertimenti originando l'esecuzione delle macro.

5. **Usate regolarmente più di un software antivirus.** Non è necessario averli tutti installati (mai installare più di uno contemporaneamente). Eseguite gli antivirus nell'opzione di scansione su richiesta, sulla cartella che contiene i files da controllare.
   Nessun antivirus può essere efficace se non l'avete aggiornato con i diversi upgrade, update o add-on. Attualmente gli aggiornamenti sono giornalieri (KAV - AVP - Panda ed altri). Non lasciate trascorrere più di 24 ore per installare gli aggiornamenti ed in ogni caso non aspettate più di una settimana per farlo. Non esistono i virus troppo nuovi e senza antivirus, la risposta dei produttori di questi software è immediata in ogni caso. Controllate che anche il vostro software risponda prontamente con aggiornamenti adeguati. Eseguite almeno una volta al mese una scansione di tutti i vostri file.

6. Considerate l'opportunità d'installare di un software di tipo **"personal firewall"** che diminuisca il rischio di troiani, virus ed altri tipi di codici dannosi che tentino una connessione da e verso il vostro PC, senza permesso. **Zone Alarm**, gratuito nella versione per uso personale, è un'eccellente scelta. Inoltre, protegge da molti dei virus che vengono trasmessi via posta elettronica, cambiando l'estensione dei file potenzialmente pericolosi, prima che arrivino alla base dati dei messaggi.

7. Preferite **l'invio** di e-mail in modo **testo**. Nascondere un virus in un file HTML è molto facile ed in certi casi si può eseguire senza doppio clic.

8. Disabilitate l'opzione "Preview" in **Outlook**. Ciò evita la visualizzazione di un messaggio fino a quando facciamo "doppio clic" su di esso. Ad ogni modo, ciò non evita l'intromissione di un virus quando apriamo il messaggio (non parliamo di un file allegato ad un messaggio, ma semplicemente della visualizzazione del testo di un messaggio). Per disabilitare l'opzione "Preview" dal menù "*Visualizza*" di Outlook, selezionate l'opzione "*Layout*" e poi deselezionate la casella "**Visualizza riquadro di anteprima**".

9. Ricordate che esiste il rischio della "**doppia estensione**". Windows, per difetto, nasconde le estensioni dei file più usati. Così un file **esempio.txt** in realtà può essere **esempio.txt.exe** o .VBS, ecc.. Questa è la forma preferita adottata da molti virus. L'estensione .VBS rimane nascosta, e pertanto sembrerà essere un file di testo: .TXT. Perché ciò non accada, disabilitate l'opzione affinché possiate vedere sempre l'estensione dei file.

   Per poter vedere le vere estensioni dei file e visualizzare le proprietà di quelli nascosti, procedete così:
   · **Windows 95**, Risorse del PC - Strumenti - Opzioni Cartella – Visualizza
   · **Windows 98**, Risorse del PC - Strumenti - Opzioni Cartella - Visualizza
   · **Windows Me**, Risorse del PC - Strumenti - Opzioni Cartella – Visualizza

   Nel menù File disabilitate la funzione "**Nascondi le estensioni dei file per i tipi di file conosciuti**" o simile. Abilitate l'opzione "**Mostra tutti i file nascosti**" o simile.

10. Se necessario, **aggiornate** la vostra versione Windows e Internet Explorer connettendovi al sito http://windowsupdate.microsoft.com/
    Selezionate "*Aggiornamenti critici*" per assicurarvi che il vostro sistema funzioni senza problemi e per proteggerlo da possibili falle di sicurezza. Un "*pacchetto di aggiornamenti critici*" appare sempre che questi siano necessari al vostro sistema. Scaricate ciò che ritenete sia necessario per aggiornare il sistema.

11. Disabilitate il **Windows Scripting Host** (WSH). Questa caratteristica può essere utile per automatizzare diverse operazioni all'interno di Windows, ma può servire anche a numerosi virus a diventare eseguibili. Per disabilitare il WSH, andate al Pannello di Controllo (Risorse del Computer, Pannello di controllo) Installazione Applicazioni, Installazione di Windows, Accessori, Dettagli, disabilitare "Windows Scripting Host". Riavviare il PC. Se si ha in uso Windows Me, usate altre opzioni come il NOSCRIPT.EXE di Symantec.

12. Per aumentare la sicurezza in Outlook, andate a Strumenti, Opzioni, selezionate "**Protezione**", nella voce "Aree di Protezione" selezionate "**Area siti con restrizione (massima protezione)**". Fate clic su "Accetta" e confermate le modifiche. Questa operazione vi proteggerà da alcuni virus.

13. Se ricevete un messaggio con l'indicazione di un virus, dove vi si chiede "inviare ai vostri indirizzi e-mail?" non fatelo. Questo tipo di virus o allarmi sono totalmente **falsi**. Ma questi messaggi attivano un tipo di "contaminazione" molto diverso, e cioè diffondono migliaia di messaggi su di essi (vengono chiamati **HOAXEs**).
    Così come può essere pericoloso credere in certi trucchi che promettono una sicurezza che non è tale (come aggiungere "**!0000**" alla rubrica) o peggio ancora, cancellare file soltanto perché qualcuno li considera dei virus (come ad esempio il **SULFNBK**).

14. Non scaricate niente dai siti web dei quali non si abbia la certezza di serietà o che non siano conosciuti. Se si decide di scaricare procedere come per i file spediti insieme all'e-mail. Copiateli in una cartella e controllateli con due o tre antivirus aggiornati prima di aprirli.

15. E' consigliabile avere un dischetto protetto per l'avvio del PC in caso di infezione. Stampate e conservate le istruzioni per eseguire l'antivirus F-PROT da un paio di dischetti. F-PROT è un antivirus gratuito se per uso personale.

16. Usate **password** articolate. Una buona password è difficile da indovinare e, se il sistema lo permette, tipicamente include lettere maiuscole e minuscole combinate e alcuni numeri (minimo 8 caratteri) .

17. **Fate regolarmente le copie dei dati.** Pianificate un backup dei dati ogni giorno e solo per quelli modificati, ed un backup del totale dei dati una volta a settimana. Verificate le copie una volta al mese.

18. Non lasciate il PC "**on-line**" quando non viene usato. Scollegate fisicamente il cavo del PC con Internet se non viene usata la connessione, anche in presenza di linea dedicata 24 ore.

19. E' sempre opportuno mantenersi *costantemente* informati sui modi di operare dei virus.