

# XP dopo l'8/04/2014

Se si vuole mantenere sul proprio pc il sistema operativo Windows XP, dall'8 Aprile 2014 si deve prendere molte precauzioni in più e non si potrà essere distratti. La cosa essenziale da capire è che l'uso del computer cambierà rispetto a prima. Anche se non si sarà sicuri al 100% (cosa impossibile anche con il miglior sistema di sicurezza del mercato a pagamento), questa piccola guida ci aiuterà a capire come difenderci (gratuitamente) da molti possibili attacchi alla nostra sicurezza.

## Limitare l'account utente

Solitamente chi sta utilizzando XP, lo fa con un account con diritti da amministratore, ciò è molto pericoloso ed è quindi giunto il momento di cambiare e limitare i permessi del proprio account. Utilizzando un account limitato con XP si dimostrerà molto noioso poiché per installare nuovi programmi dovrete sempre accedere con l'account amministratore.

## Installare un ottimo antivirus

Cosa che in realtà era necessaria anche prima dell'8 aprile e quindi è quindi non sarà una novità.

Tra quelli gratuiti potete scegliere AVG, Avast, Avira, Bitdefender, ESET, F-Secure, G Data o Kaspersky, Sophos e Trend Micro...le scelte non mancano.

## Installare un ottimo firewall

Il firewall è uno strumento necessario su un sistema operativo, in assenza di aggiornamenti per la sicurezza, rimanendo sempre più soggetto ad attacchi di hacker che sicuramente proveranno a cercare le vulnerabilità di questo sistema non più supportato.

## Disattivare il Remote Desktop

Cliccare su "Start", scegliere "Pannello di controllo" e la voce "Sistema", nella scheda "Connessione remota", deselezionare l'opzione "Consenti agli utenti di connettersi in remoto al tuo computer" e fai click su "OK". Così facendo andiamo a rendere immune da eventuali attacchi questo vulnerabile protocollo RDP (Remote Desktop Protocol) e il computer diventa un po' più sicuro.

## PC con Windows XP e internet

Se volete continuare ad usare il vostro pc navigando in Internet, allora sul nostro Windows XP dovremo installare l'ultima versione di un browser come Google Chrome ed evitare quelli più pericolosi come Internet Explorer e Firefox, poiché non supportano più il nostro sistema operativo. Bisogna aggiornare i plug-in del browser ed evitare di installare estensioni non garantite al 100%.

## Usare Sandboxie

Sandboxie è un'applicazione molto utile e crea una zona protetta sul sistema dove anche un virus sarebbe isolato dal resto dei software installati. Si utilizzerà ogni volta che si installerà un nuovo programma e che si vorrà navigare su un sito di cui non si è sicuri.

## Creare un kit di emergenza

Per aumentare ancora la nostra sicurezza, nell'ultimo paragrafo di questa nostra piccola guida, vi vogliamo suggerire la creazione di un "kit di emergenza" (magari messo in una cartella, o in una memoria USB) con all'interno una serie di antivirus, che possano essere utilizzati ogni tanto, per controllare il nostro sistema.

Tra quelli che vi consigliamo ci sono:

ClamWin, SuperAntiSpyware, Kaspersky Virus Removal Tool, Microsoft Safety Scanner, Emsisoft Antivirus e NoVirusThanks.

Questi programmi antivirus che abbiamo appena elencato possiedono tutti una versione portable (portatile) che può essere molto utile in caso un virus, o altri "agenti esterni" si siano infiltrati nel nostro sistema.

