LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

# Come proteggere il browser da pubblicità indesiderata e reindirizzamenti

Autore: Redazione | 07/05/2019

***Il tuo dispositivo è costantemente rallentato da pubblicità non richieste e da continui reindirizzamenti? In questa guida ti forniamo alcuni semplici ed efficaci strumenti per migliorare la tua sicurezza e la qualità***

*della tua navigazione su Internet.*

Con l'evoluzione della tecnologia e di Internet, la navigazione sui nostri portali preferiti è diventata sempre più difficoltosa, portandoci a fare un vero e proprio slalom fra banner pubblicitari, pop-up e reindirizzamenti non richiesti. Se da un lato questa pratica, nota con il termine adware, è in parte motivata dalla necessità di assicurare ai portali web l'introito minimo per sostentare il sito, dall'altro espone i nostri computer e i nostri smartphone a pericoli di sicurezza, rendendoli inoltre decisamente più lenti e instabili. Se la misura per te è ormai colma, e hai intenzione di dare una svolta alla tua esperienza di navigazione, sei capitato nel posto giusto. Nelle prossime righe ti spiegheremo infatti **come proteggere il browser da pubblicità indesiderata e reindirizzamenti**, fornendoti tutte le indicazioni necessarie per azzerare le attività da te non autorizzate sul tuo computer o sul tuo dispositivo mobile.

# Cos'è un adware?

Prima di procedere oltre, partiamo dalle basi. L'**adware** è un software ideato e realizzato in modo tale da lanciare **messaggi pubblicitari** sullo schermo. Questo può essere fatto sia attraverso un **browser** internet, sia all'interno di un programma o di un'**app**.

Le **pubblicità a schermo** durante la visualizzazione dei nostri siti web preferiti fanno ormai parte della nostra esistenza e del nostro tempo libero, ma vale la stessa cosa anche per le app che scarichiamo, che, in particolare nelle loro versioni gratuite, si assicurano introiti attraverso il lancio di brevi **spot promozionali** o l'inserimento di **banner pubblicitari** all'interno dell'interfaccia.

Esistono attività decisamente più subdole che possono minare alla base il funzionamento dei nostri dispositivi. Ci riferiamo all'apertura di diverse schede sul browser che utilizzi, l'impostazione di un determinato indirizzo web come home page dello stesso o il reindirizzamento forzato ad altri portali, che spesso e volentieri ospitano al loro interno contenuti pornografici o fraudolenti. Le attività potenzialmente pericolose non si fermano però qui. In maniera similare a un tradizionale **virus informatico**, l'adware può penetrare all'interno del nostro sistema e cominciare a raccogliere preziosi dati su di noi, come le nostre attività, le nostre preferenze o addirittura la geolocalizzazione delle nostre posizioni. Gli

**sviluppatori di adware** possono poi vendere queste informazioni a terzi o utilizzarle per proporci annunci pubblicitari in linea con le nostre preferenze, aumentando di conseguenza ulteriormente i loro profitti.

# Sei vittima di un adware?

Potresti essere vittima di un adware se hai notato uno o più di questi comportamenti anomali sul tuo computer o sul tuo dispositivo mobile:

- comparsa di **annunci pubblicitari** in posizioni diverse dal solito;
- cambio non autorizzato dell'**home page** di uno o più browser;
- **anomalie** nella consultazione di **siti web** che frequenti abitualmente;
- continui **reindirizzamenti** a link diversi da quelli da te richiesti;
- browser estremamente lento su diverse **pagine web**;
- comparsa improvvisa e non autorizzata di nuove toolbar, estensioni o plugin all'interno del tuo browser;
- avvio automatico e non autorizzato di **installazione di applicazioni**;
- blocco improvviso del browser durante la navigazione.

Come abbiamo visto, un adware può infiltrarsi nel tuo dispositivo in molteplici modi. Puoi per esempio avere scaricato un **software** o un'**app freeware**, che ha però installato a sua volta un altro programma (è questo il caso delle fastidiose **toolbar**, la cui rimozione comporta spesso diverse difficoltà).

Puoi esserti imbattuto in un **drive-by download**, ovvero l'installazione da un sito malevolo di un software capace di tracciare le tue informazioni, indirizzandoti di conseguenza verso altri siti fraudolenti che potrebbero attirare la tua attenzione o proponendoti annunci pubblicitari potenzialmente in linea con i tuoi **interessi** durante la **navigazione su interne**t.

A prescindere dalla modalità con cui sei stato colpito, devi innanzitutto rivedere le tue **abitudini sul web**, limitando al minimo indispensabile la consultazione di siti internet della cui affidabilità non sei certo, prestando particolare attenzione al download e all'installazione di app o programmi gratuiti e non cliccando su banner pubblicitari potenzialmente fraudolenti, come il classico "Congratulazioni, sei il milionesimo cliente!".

In secondo luogo, per salvaguardare la **sicurezza** del tuoi dispositivi e dei tuoi dati

personali, è opportuno procedere al download di un **software** che elimini gli adware sul tuo computer o sul tuo smartphone e che contemporaneamente impedisca l'installazione degli stessi. Nel prosieguo dell'articolo, cercheremo di darti qualche indicazione in questo senso, ma ci teniamo a sensibilizzarti sul fatto che il primo difensore dei tuoi dati e del tuo hardware devi essere sempre e comunque tu, attraverso una gestione oculata delle tue **attività online**.

# Programmi per eliminare gli Adware

Il primo software per **rimuovere gli adware** che ti consigliamo è **MalwareBytes**, disponibile per Windows, Mac, Android e iOS. In tutte le sue versioni, questo software permette di eliminare la totalità degli adware presenti nel dispositivo che lo sta ospitando.

La **versione a pagamento di MalwareBytes** permette inoltre di prevenire l'installazione degli stessi, attraverso un monitoraggio in tempo reale che elimina alla radice anche virus, **spyware** e **ransomware**. La **versione gratuita** del programma è comunque in grado di aiutarti per il tuo problema principale, ovvero la rimozione degli adware che malauguratamente sono già stati installati sul tuo computer. Per mettere in pratica questa procedura, procedi come segue. Innanzitutto, **scarica il software** da uno dei quattro link che ti abbiamo fornito poche righe sopra, in base al sistema operativo fisso o mobile che stai utilizzando. In secondo luogo, procedi all'**installazione del programma** o dell'**app**, che non richiede alcuna spiegazione particolare (accetta tutto quello che ti viene chiesto e, se richiesto, inserisci la tua password di amministratore).

Una volta installato MalwareBytes, puoi procedere alla **scansione**, cliccando sul pulsante Esegui la scansione ora, che trovi nell'interfaccia principale del programma. A questo punto, partirà una **procedura** che scandaglierà attentamente il tuo dispositivo, alla ricerca di file o programmi potenzialmente malevoli. Al termine di questa attività, ti verranno fornite tutte le indicazioni necessarie per risolvere gli eventuali problemi rilevati, come la quarantena o l'eliminazione di determinati file o programmi. Se non sei sicuro al 100% dell'**affidabilità dei software** rilevati come malevoli, fidati del programma ed effettua tutte le operazioni richieste.

Se sei soddisfatto del risultato, puoi procedere all'attivazione della **protezione** in tempo reale per un periodo di prova gratuita di 14 giorni, al termine dei quali

dovrai **acquistare una licenza** di MalwareBytes per continuare a beneficiare del servizio. Per **attivare la prova gratuita**, ti basta fare un clic su Attiva la protezione nella schermata principale di MalwareBytes. Puoi inoltre osservare in qualsiasi momento ciò che il programma ha eseguito sul tuo dispositivo semplicemente selezionando la scheda Report, all'interno della quale avrai un quadro preciso delle azioni messe in piedi per **tutelare la tua privacy** e la tua **sicurezza**.

Un altro prezioso supporto nella lotta contro gli adware è indubbiamente quello fornito da **Avast Security**, celebre **antivirus**, disponibile sia per Windows che per Mac, che permette di difendersi anche da queste specifiche minacce. Anche questo programma prevede l'acquisto di una licenza, tuttavia la versione gratuita dello stesso è più che sufficiente per contrastare gli adware.

Per cominciare a proteggerti, recati sul sito ufficiale di Avast e procedi al download della versione del programma compatibile con il sistema operativo che stai utilizzando in questo momento. Prima di procedere oltre, assicurati di rimuovere dal tuo sistema altri antivirus, che Avast potrebbe erroneamente considerare come minacce. Sarà comunque lo stesso programma a proporti la rimozione di altri software, giudicati non compatibili.

Una volta terminato il download di Avast, procedi con l'installazione, che non richiede alcuna particolare abilità. Assicurati soltanto di rifiutare, nel caso in cui tu non sia interessato, eventuali installazioni di software aggiuntivi che Avast potrebbe proporti durante la **procedura di inizializzazione dell'antivirus**. A seconda del tuo sistema operativo e delle tue attuali impostazioni di sicurezza, Avast potrebbe inoltre richiederti alcune specifiche **autorizzazioni** per poter cominciare il suo lavoro di protezione del tuo sistema; per concederle, segui ciò che ti viene indicato dallo stesso programma con dovizia di particolari, con la consapevolezza che tutto ciò avviene per fornirti un maggior livello di sicurezza durante la tua **navigazione**.

Al termine dell'installazione, ti sarà possibile eseguire la prima **scansione** del tuo sistema. Per farlo, devi soltanto fare clic su Scansiona all'interno dell'interfaccia principale del programma, selezionando successivamente l'opzione Scansione sistema completo per un'analisi più approfondita delle eventuali minacce installate sul tuo sistema. Attendi quindi qualche minuto per avere il responso dell'attività eseguita da parte di Avast. A questo punto, non ti resta che riporre la tua fiducia

nelle azioni consigliate dal **programma** e seguirle scrupolosamente per eliminare le minacce installate sul tuo sistema.

Avast Security ti fornirà inoltre alcuni **consigli** per aumentare lo spazio a disposizione sul tuo computer, attraverso la **cancellazione di file** ritenuti inutili. In questo specifico caso, prima di dare il tuo consenso a questa operazione, assicurati di non autorizzare l’eliminazione di file che desideri conservare.