

Google reCaptcha

L'**indirizzo IP pubblico**, se non ne avessi mai sentito parlare, è una sequenza di numeri (e lettere, se si parla di IPv6), mediante la quale ciascun router, smartphone, tablet e, in generale, qualsiasi dispositivo connesso viene identificato su Internet. In soldoni, l'indirizzo IP serve a identificare con precisione un dispositivo collegato a Internet e a far sì che i dati possano viaggiare con esattezza tra i vari device connessi alla grande rete.

Alcuni server, ma anche alcuni PC su cui sono presenti determinati programmi, possono essere impiegati per eseguire delle operazioni poco "lecite", come l'invio di **spam** o l'**esecuzione automatica di operazioni sequenziali**.

Quando questi dispositivi vengono stanati, i relativi indirizzi IP vengono segnalati come potenziali robot (o "**bot**") e inseriti in una o più **blacklist**: queste ultime vengono utilizzate da vari servizi online, tra cui Google, per avere un'idea degli indirizzi innocui e di quelli potenzialmente nocivi e mettere a punto delle opportune strategie di difesa.

Se si visita una piattaforma da un indirizzo IP potenzialmente appartenente a un **bot**, essa può rispondere in modo differente: nel caso di Google, viene effettuato il famoso controllo di sicurezza "**Non sono un robot**", che consiste nel **selezionare una o più immagini contenenti elementi ben definiti** da una serie di foto, oppure di **centrare una casella di controllo** posta solitamente in alto. In tal modo, il motore di ricerca riesce ad accertarsi che quell'indirizzo IP è al momento usato da un essere umano e che, almeno in linea teorica, non è nocivo.

Tuttavia, superare il controllo "Non sono un robot" non significa che l'indirizzo IP venga eliminato dalle blacklist, anzi: bastano davvero poche operazioni "strane" per finire nella lista nera degli indirizzi sospetti, ma uscirvi definitivamente è estremamente difficile, se non impossibile in alcuni casi.

Per verificare se la comparsa del controllo di sicurezza di Google è causata dalla presenza del tuo IP in una blacklist, puoi controllare su [questo sito Web](#), premendo sul pulsante **Check My IP Address**.

Dopo alcuni secondi, dovresti visualizzare il risultato dell'analisi: qualora il tuo IP fosse "pulito", tutti i risultati saranno contrassegnati da una **spunta verde**; altrimenti vedrai comparire una **X rossa** in corrispondenza della blacklist in cui esso compare.

Qualora il controllo desse esito positivo, è molto difficile che Google smetta di mostrarti la richiesta di verifica anti-robot. Tuttavia, puoi prendere una serie di accorgimenti per tentare di migliorare la situazione ed evitare la comparsa del fastidioso messaggio.

Se hai un indirizzo IP di tipo **dinamico, disconnettiti da Internet, disattivando la connessione dati** del cellulare/tablet oppure **spegnendo il router**, e riconnettiti dopo circa dieci minuti: a seguito di questa operazione, il tuo indirizzo cambierà e non dovresti più visualizzare il controllo di sicurezza su Google.

Se hai un indirizzo IP di tipo **statico, contatta il tuo provider di servizi Internet** e, dopo aver spiegato il tuo problema, concorda con quest'ultimo una soluzione da applicare. Nella maggior parte dei casi, sarà il gestore ad accertarsi della presenza dell'indirizzo IP nelle varie blacklist e, se questa non è giustificata da effettive violazioni, richiederne l'eliminazione

potresti aver contratto un **trojan** ed essere finito in una **botnet**, ossia in un sistema di computer collegati che, all'oscuro dell'utente, svolgono operazioni illecite.

In altre parole, potresti essere stato usato inconsapevolmente come **bot** e Google, ahimè, potrebbe averti scoperto e contrassegnato come indirizzo potenzialmente dannoso.

In casi come questo, il primo step da compiere è verificare la presenza di eventuali **estensioni sospette** nel **browser** del computer e disattivarle immediatamente: per procedere, se impieghi **Google Chrome** o **Microsoft Edge**, clicca sul simbolo del **puzzle** che risiede in alto a destra (su Chrome) oppure sull'icona [...] (su Edge) e poi sulla voce **Gestisci estensioni**, situata nel menu che compare. Ora, utilizza la nuova scheda visualizzata per cercare eventuali componenti aggiuntivi a te sconosciuti e, se li trovi, **rimuovili** subito cliccando sull'apposito pulsante o sulla voce dedicata .

Su **Firefox**, invece, devi cliccare sull'icona ≡ collocata in alto a destra e poi sulla voce **Componenti aggiuntivi** situata nel menu che compare: se noti qualche estensione che non dovrebbe essere lì, clicca prima sul pulsante [...] corrispondente al suo riquadro e poi sulla voce **Rimuovi**, che compare nel menu visualizzato.

Se il tuo browser è **Safari**, invece, recati nel menu **Safari > Preferenze** (si trova in alto a sinistra), seleziona la scheda **Estensioni** nella finestra che si apre e, dopo aver individuato il componente aggiuntivo "sospetto", selezionalo con un clic e premi il pulsante **Rimuovi**. Ti faccio comunque presente che l'eventualità di incappare in componenti aggiuntivi e/o toolbar nocivi, su Mac, è decisamente rara.