Qual è il miglior browser per non essere tracciati

Maria Cattini | 23/04/2026 | Sicurezza digitale

Apri il browser, fai una ricerca, scorri due siti. Dopo pochi minuti, gli annunci ti seguono ovunque.

Non è una coincidenza. È tracciamento.

E qui nasce il primo errore: pensare che basti “un browser giusto” per sparire.

Non funziona così.

Cosa significa “non essere tracciati”

Ci sono due livelli diversi — e confonderli crea false sicurezze:

• Privacy → bloccare pubblicità e profilazione
• Anonimato → nascondere chi sei e da dove ti connetti

Sono due cose diverse.

Un browser può aiutarti sul primo livello.
Sul secondo, serve molto di più.

Il punto chiave: **nessun browser ti rende invisibile da solo**

I browser più efficaci oggi

1. Tor Browser → anonimato reale

• Nasconde l’IP
• Instrada il traffico su più nodi
• Isola ogni sito

Risultato: difficile collegare le tue attività a te

□□ Problema concreto:

• lento
• molti siti non funzionano
• spesso bloccato

Non è un browser “comodo”.
È uno strumento da usare quando serve davvero.

2. Brave → protezione immediata

• Blocca tracker e pubblicità senza plugin
• Riduce fingerprinting (impronta digitale del browser)
• Funziona subito, senza configurazioni

Test indipendenti mostrano blocchi fino al ~97% dei tracker

□□ Tradotto: meno profilazione, meno pubblicità mirata

3. Firefox (configurato) / LibreWolf → controllo totale

• Firefox base: buona protezione
• Firefox “hardenizzato”: livello alto
• LibreWolf: già pronto, senza telemetria

Blocchi intorno al 90%+ nei test

□□ Differenza reale:

• più controllo
• più lavoro manuale

Parte operativa: come scegliere il browser

STEP 1 — Definisci cosa stai proteggendo

Fai questa domanda:

• vuoi evitare pubblicità? → Brave
• vuoi anonimato serio? → Tor
• vuoi controllo tecnico? → Firefox / LibreWolf

□□ Senza questo passaggio, scegli a caso.

STEP 2 — Imposta un uso separato

Errore tipico: usare lo stesso browser per tutto.

Fai così:

• Browser 1 → uso quotidiano (email, social)
• Browser 2 → ricerche sensibili
• Browser 3 (Tor) → attività delicate

□□ Questo riduce collegamenti tra sessioni

STEP 3 — Disattiva il tracciamento “interno”

Anche il browser più sicuro perde valore se:

• sei loggato su Google
• sei loggato su Facebook
• sincronizzi tutto

□□ Azione concreta:

• usa profili separati
• evita login inutili

STEP 4 — Blocca fingerprinting e script

Se usi Firefox:

• installa uBlock Origin
• attiva protezione avanzata
• disattiva WebRTC

Se usi Brave:

• attiva Shields su “aggressivo”

□□ Questo riduce l’identificazione invisibile

STEP 5 — Non fidarti solo del browser

Il tracciamento passa anche da:

• IP (provider internet)
• comportamento
• account

□□ Se serve anonimato reale:

• usa Tor
• oppure VPN + browser configurato

Caso concreto (reale e replicabile)

Scenario:

> Vuoi cercare informazioni su un’azienda senza essere profilato.

Metodo:

1. Apri Tor Browser
2. Non fare login da nessuna parte
3. Cerca il nome azienda
4. Apri risultati in nuove schede isolate
5. Evita download o interazioni

Risultato:

• nessun collegamento diretto con il tuo IP
• attività difficile da correlare

Errore comune (da evitare subito)

□□ Pensare: “uso Brave → sono anonimo”

No.

Brave riduce il tracciamento pubblicitario.
Non nasconde la tua identità di rete.

Questa confusione è la più diffusa — e la più pericolosa.

Cosa evitare

• Chrome / Edge senza configurazioni
• estensioni casuali (spesso tracciano)
• usare sempre lo stesso browser per tutto

Con Manifest V3, molti browser limitano gli ad-blocker

□□ Tradotto: meno controllo, più esposizione

Il punto che cambia tutto

Non esiste “il browser migliore”.

Esiste **il browser giusto per il tuo scenario**.

• Investigazione → Tor
• Uso quotidiano → Brave
• Controllo avanzato → Firefox / LibreWolf

Risultato atteso

Se applichi questi passaggi:

• riduci drasticamente la profilazione
• separi le attività
• eviti correlazioni tra sessioni

Non diventi invisibile.

Ma smetti di essere un bersaglio facile.

La privacy non si compra con un download. Si costruisce con scelte precise. Il browser è solo il primo passo.

Entra nella community

Newsletter → https://coondivido.substack.com/

Telegram → https://t.me/osintaipertutti

Telegram → https://t.me/osintprojectgroup

Apri il browser, fai una ricerca, scorri due siti. Dopo pochi minuti, gli annunci ti seguono ovunque.

Non è una coincidenza. È tracciamento.

E qui nasce il primo errore: pensare che basti “un browser giusto” per sparire.

Non funziona così.

Cosa significa “non essere tracciati”

Ci sono due livelli diversi — e confonderli crea false sicurezze:

• Privacy → bloccare pubblicità e profilazione
• Anonimato → nascondere chi sei e da dove ti connetti

Sono due cose diverse.

Un browser può aiutarti sul primo livello.
Sul secondo, serve molto di più.

Il punto chiave: **nessun browser ti rende invisibile da solo**

I browser più efficaci oggi

1. Tor Browser → anonimato reale

• Nasconde l’IP
• Instrada il traffico su più nodi
• Isola ogni sito

Risultato: difficile collegare le tue attività a te

□□ Problema concreto:

• lento
• molti siti non funzionano
• spesso bloccato

Non è un browser “comodo”.
È uno strumento da usare quando serve davvero.

2. Brave → protezione immediata

• Blocca tracker e pubblicità senza plugin
• Riduce fingerprinting (impronta digitale del browser)
• Funziona subito, senza configurazioni

Test indipendenti mostrano blocchi fino al ~97% dei tracker

□□ Tradotto: meno profilazione, meno pubblicità mirata

3. Firefox (configurato) / LibreWolf → controllo totale

• Firefox base: buona protezione
• Firefox “hardenizzato”: livello alto
• LibreWolf: già pronto, senza telemetria

Blocchi intorno al 90%+ nei test

□□ Differenza reale:

• più controllo
• più lavoro manuale

Parte operativa: come scegliere il browser

STEP 1 — Definisci cosa stai proteggendo

Fai questa domanda:

• vuoi evitare pubblicità? → Brave
• vuoi anonimato serio? → Tor
• vuoi controllo tecnico? → Firefox / LibreWolf

□□ Senza questo passaggio, scegli a caso.

STEP 2 — Imposta un uso separato

Errore tipico: usare lo stesso browser per tutto.

Fai così:

• Browser 1 → uso quotidiano (email, social)
• Browser 2 → ricerche sensibili
• Browser 3 (Tor) → attività delicate

□□ Questo riduce collegamenti tra sessioni

STEP 3 — Disattiva il tracciamento “interno”

Anche il browser più sicuro perde valore se:

• sei loggato su Google
• sei loggato su Facebook
• sincronizzi tutto

□□ Azione concreta:

• usa profili separati
• evita login inutili

STEP 4 — Blocca fingerprinting e script

Se usi Firefox:

• installa uBlock Origin
• attiva protezione avanzata
• disattiva WebRTC

Se usi Brave:

• attiva Shields su “aggressivo”

□□ Questo riduce l’identificazione invisibile

STEP 5 — Non fidarti solo del browser

Il tracciamento passa anche da:

• IP (provider internet)
• comportamento

• account

□□ Se serve anonimato reale:

• usa Tor
• oppure VPN + browser configurato

Caso concreto (reale e replicabile)

Scenario:

> Vuoi cercare informazioni su un’azienda senza essere profilato.

Metodo:

1. Apri Tor Browser
2. Non fare login da nessuna parte
3. Cerca il nome azienda
4. Apri risultati in nuove schede isolate
5. Evita download o interazioni

Risultato:

• nessun collegamento diretto con il tuo IP
• attività difficile da correlare

Errore comune (da evitare subito)

□□ Pensare: “uso Brave → sono anonimo”

No.

Brave riduce il tracciamento pubblicitario.
Non nasconde la tua identità di rete.

Questa confusione è la più diffusa — e la più pericolosa.

Cosa evitare

• Chrome / Edge senza configurazioni
• estensioni casuali (spesso tracciano)
• usare sempre lo stesso browser per tutto

Con Manifest V3, molti browser limitano gli ad-blocker

□□ Tradotto: meno controllo, più esposizione

Il punto che cambia tutto

Non esiste “il browser migliore”.

Esiste **il browser giusto per il tuo scenario**.

• Investigazione → Tor
• Uso quotidiano → Brave
• Controllo avanzato → Firefox / LibreWolf

Risultato atteso

Se applichi questi passaggi:

• riduci drasticamente la profilazione
• separi le attività
• eviti correlazioni tra sessioni

Non diventi invisibile.

Ma smetti di essere un bersaglio facile.

La privacy non si compra con un download. Si costruisce con scelte precise. Il browser è solo il primo passo.

Entra nella community

Newsletter → https://coondivido.substack.com/

Telegram → https://t.me/osintaipertutti

Telegram → https://t.me/osintprojectgroup