□□ I browser più sicuri del 2025: guida pratica per scegliere quello giusto

Maria Cattini | 16/04/2025 | Sicurezza digitale

□□ Browser sicuri? Come scegli il browser oggi?

C’è stato un tempo in cui bastava **installare Chrome o Firefox**, e si era pronti a navigare. Oggi non è più così. Con l’aumento di:

• tracciamenti invisibili,
• AI che analizzano le nostre abitudini digitali,
• attacchi di phishing iper-personalizzati,
• e vere e proprie campagne di sorveglianza digitale,

la scelta del browser non è più solo una questione di gusti, ma una vera e propria decisione strategica di sicurezza personale.

□□ Perché la sicurezza del browser è una priorità (anche per chi usa OSINT)

Se operi nel mondo dell’**Open Source Intelligence**, fai **ricerche sensibili** o semplicemente vuoi proteggere i tuoi dati, il browser che usi è **il tuo primo alleato… o il tuo peggior nemico**.

Ecco perché abbiamo analizzato e confrontato i **6 browser più sicuri del 2025**, per aiutarti a scegliere il migliore in base al tuo profilo.

□□ Tabella comparativa: browser sicuri 2025

Browser	Motore	Open Source	Blocco Ads	VPN integrata	Estensioni	Punti di forza
Brave	Chromium	□	□	□	□	Blocco nativo tracker e ads, compatibile con Chrome.
LibreWolf	Gecko (Firefox)	□	□	□	□	Privacy estrema, no telemetria, uBlock Origin preinstallato.
Tor Browser	Gecko (Tor)	□	□	□ (via Tor)	□	Navigazione anonima via rete Tor.
Vivaldi	Chromium	□	□	□ (Proton)	□	Personalizzabile, VPN + mail + calendario

Browser	Motore	Open Source	Blocco Ads	VPN integrata	Estensioni	Punti di forza
Opera	Chromium	✅	✅	✅ (limitata)	✅	Facile da usare, sidebar social, VPN inclusa.
Falkon	QtWebEngine	✅	✅	❌	❌	Super leggero, ma poco aggiornato.

🛡️ Analisi dettagliata dei browser più sicuri

🦁 Brave

Brave blocca **tracker, fingerprint e cookie** di terze parti già al primo avvio. Supporta la rete **Tor** in modalità incognito, sebbene non quanto il vero Tor Browser. Ideale per chi vuole sicurezza e velocità, **senza rinunciare alle estensioni**.

Adatto per: utenti generici, OSINT di base, giornalisti.

🐺 LibreWolf

Versione ultra-sicura di Firefox, con **tutti i componenti di tracciamento disattivati**. Nessuna telemetria, aggiornamenti frequenti, supporto estensioni. Non raccoglie **nulla**.

Adatto per: attivisti, ricercatori OSINT, esperti privacy.

🕵️‍♂️ Tor Browser

Il **gold standard** dell'anonimato. Ogni connessione è instradata su più nodi crittografati. Nessuna estensione, lentezza accettabile per il livello di protezione offerto.

Adatto per: investigazioni sensibili, navigazione nascosta, whistleblower.

🎨 Vivaldi

Non è open-source, ma offre strumenti avanzati: **client email integrato, VPN Proton**, lettore RSS, temi personalizzati. Molto amato da utenti avanzati.

Adatto per: utenti power-user, giornalisti, chi vuole controllo su ogni aspetto.

🔴 Opera

Facile da usare, include **VPN gratuita (limitata)**, blocco pubblicità e sidebar per WhatsApp/Telegram. Non è open-source, ma offre **buona protezione per uso quotidiano**.

Adatto per: utenti non esperti, adolescenti, utenti social.

🦅 Falko

Browser leggerissimo, basato su Qt e progettato per consumare poche risorse. **Non ha VPN né estensioni**, ed è aggiornato raramente.

Adatto per: sistemi obsoleti, laboratori, test ambienti chiusi.

🧪 Come testare il tuo browser

Vuoi sapere quanto è sicuro il tuo browser? Ecco tre test essenziali:

1. PrivacyTests.org

Analizza i browser in base a decine di metriche di privacy.

2. Cover Your Tracks (EFF)

Valuta fingerprint, blocco tracciatori e compatibilità con l’anonimato.

3. DNS Leak Test

Verifica se il tuo DNS espone la tua identità reale, anche con VPN attiva.

⚙ Bonus: impostazioni consigliate

Per aumentare la sicurezza del browser che già usi:

• Disattiva WebRTC
• Usa estensioni come uBlock Origin, Privacy Badger, HTTPS Everywhere
• Naviga in modalità incognito per ricerche OSINT mirate
• Imposta DNS su Cloudflare o NextDNS
• Blocca il fingerprint con CanvasBlocker

□□ Browser sicuro = indagine OSINT sicura

Chi lavora con **fonti aperte** e fa ricerca OSINT dovrebbe usare **Tor o LibreWolf**, impostando un profilo browser **dedicato all’indagine** per evitare contaminazioni con l’uso personale.

□□*Mai usare lo stesso browser per OSINT e social network personali.*

□□ Le false promesse della navigazione "anonima"

□□ Finestra in incognito: utile ma non sufficiente

Quando apri una **finestra in incognito** su Chrome, Brave o Firefox, ti senti più sicuro. Ma è davvero così?

La risposta è: **ni**.

Queste modalità, spesso chiamate “private” o “anonime”, **non nascondono la tua identità al provider internet o ai siti che visiti**. Chi gestisce il server web sa **esattamente da dove vieni, cosa cerchi e che tipo di dispositivo usi**.

Quindi, a cosa servono?

□ **Eliminano automaticamente la cronologia di navigazione e i cookie al termine della sessione.**
□ **Impediscono ad altri siti, successivamente, di usare quei cookie per tracciarti.**

□□*Sono utili per evitare che altri utenti del tuo computer vedano la tua attività, non per proteggerti dal tracciamento esterno.*

□□ Il nemico invisibile: il fingerprinting

OItre a cookie e tracciatori, c’è una tecnica ancora più subdola e invisibile: il **browser**

fingerprinting.

Questa tecnica raccoglie **dati unici sul tuo browser e dispositivo** per costruire un profilo che ti identifica online anche **senza login o cookie**.

□□ Cosa raccoglie il fingerprinting?

• Risoluzione dello schermo
• Font installati
• Fuso orario
• Sistema operativo
• Plugin attivi
• Lingua del browser
• Versione JavaScript supportata
• …e molto altro.

□□ Quando queste informazioni vengono combinate, il risultato è una **"impronta digitale"** unica. Anche se non conoscono il tuo nome, **sanno che sei "tu"**.

⚠ A chi serve?

• □□□□ Agli inserzionisti: per proporti pubblicità personalizzate
• □□♂ Alle piattaforme di analytics: per tracciare comportamenti
• □□□□ Anche a chi ha intenzioni meno legittime

□□ Come difendersi dal fingerprinting?

• Usa browser come LibreWolf o Tor, che limitano l'entropia delle informazioni trasmesse.
• Installa estensioni come CanvasBlocker, Trace o NoScript.
• Disattiva WebGL, WebRTC e i font personalizzati (se non ti servono).
• Modifica l'user agent del browser con strumenti come User-Agent Switcher.

□□ Ricorda: nessun sistema è perfetto. Ma **ridurre il livello di dettaglio trasmesso** è già un grande passo per la tua privacy.

□□ Vuoi approfondire?

• Prova LibreWolf per una privacy totale.
• Scarica Brave per una protezione immediata.
• Avvia le tue indagini su Tor Browser in totale anonimato.

□□ Hai dubbi o vuoi condividere le tue impostazioni ideali? Scrivici su Telegram o unisciti alla nostra newsletter!

I browser più sicuri del 2025

- **Combatti tracker e phishing,** quale il browser che scegii è strategico per bloccare tracciamenti invisibili è phishingg mirato.
- Ab**biamo testato** i 8 browser più sicuri del 2025: vediamo qual è il migllore per te.

Tabella comparativa

Browser	Blocco traccianti	VPN	Open Source
Brave	✓	✓	✓
LibreWolf	✓	✓	✓
Tor Browser	✓	✓	✓
Vivaldi	✓	✓	✗
Opera	✓	✗	✗

Testati: pro e contro

+ Blocco nativo tracker e ads

– Non completamente anonimo

+ Privacy estrema, no telemetria

– Navigazione anonima via rete Tor

– Vinií Proton e funzionalità avanzate

+ Facile da usare, siubarsocial

– VPN limitata e chiusa

Come difendertidi più

- Web in incognito non significa web anonimo! Usa Tor o LibréWolf per più protezione
- Installa estensioni anti-tracker come uBlock Origin
- Disabilita WebRTC per evitare “DNS leak”

→ **Guida completa su:**

coondivido.it/browser-sicuri-2025

□□ Browser sicuri? Come scegli il browser oggi?

C’è stato un tempo in cui bastava **installare Chrome o Firefox**, e si era pronti a navigare. Oggi non è più così. Con l’aumento di:

• tracciamenti invisibili,
• AI che analizzano le nostre abitudini digitali,
• attacchi di phishing iper-personalizzati,
• e vere e proprie campagne di sorveglianza digitale,

la scelta del browser non è più solo una questione di gusti, ma una vera e propria decisione strategica di sicurezza personale.

□□ Perché la sicurezza del browser è una priorità (anche per chi usa OSINT)

Se operi nel mondo dell’**Open Source Intelligence**, fai **ricerche sensibili** o semplicemente vuoi proteggere i tuoi dati, il browser che usi è **il tuo primo alleato… o il tuo peggior nemico**.

Ecco perché abbiamo analizzato e confrontato i **6 browser più sicuri del 2025**, per aiutarti a scegliere il migliore in base al tuo profilo.

□□ Tabella comparativa: browser sicuri 2025

Browser	Motore	Open Source	Blocco Ads	VPN integrata	Estensioni	Punti di forza
Brave	Chromium	□	□	□	□	Blocco nativo tracker e ads, compatibile con Chrome.
LibreWolf	Gecko (Firefox)	□	□	□	□	Privacy estrema, no telemetria, uBlock Origin preinstallato.
Tor Browser	Gecko (Tor)	□	□	□ (via Tor)	□	Navigazione anonima via rete Tor.
Vivaldi	Chromium	□	□	□ (Proton)	□	Personalizzabile, VPN + mail + calendario integrati.
Opera	Chromium	□	□	□ (limitata)	□	Facile da usare, sidebar social, VPN inclusa.
Falkon	QtWebEngine	□	□	□	□	Super leggero, ma poco aggiornato.

□□ Analisi dettagliata dei browser più sicuri

□□ Brave

Brave blocca **tracker, fingerprint e cookie** di terze parti già al primo avvio. Supporta la rete **Tor** in

modalità incognito, sebbene non quanto il vero Tor Browser. Ideale per chi vuole sicurezza e velocità, **senza rinunciare alle estensioni**.

Adatto per: utenti generici, OSINT di base, giornalisti.

□□ LibreWolf

Versione ultra-sicura di Firefox, con **tutti i componenti di tracciamento disattivati**. Nessuna telemetria, aggiornamenti frequenti, supporto estensioni. Non raccoglie **nulla**.

Adatto per: attivisti, ricercatori OSINT, esperti privacy.

□□♂ Tor Browser

Il **gold standard** dell'anonimato. Ogni connessione è instradata su più nodi crittografati. Nessuna estensione, lentezza accettabile per il livello di protezione offerto.

Adatto per: investigazioni sensibili, navigazione nascosta, whistleblower.

□□ Vivaldi

Non è open-source, ma offre strumenti avanzati: **client email integrato, VPN Proton**, lettore RSS, temi personalizzati. Molto amato da utenti avanzati.

Adatto per: utenti power-user, giornalisti, chi vuole controllo su ogni aspetto.

□□ Opera

Facile da usare, include **VPN gratuita (limitata)**, blocco pubblicità e sidebar per WhatsApp/Telegram. Non è open-source, ma offre **buona protezione per uso quotidiano**.

Adatto per: utenti non esperti, adolescenti, utenti social.

□□ Falko

Browser leggerissimo, basato su Qt e progettato per consumare poche risorse. **Non ha VPN né estensioni**, ed è aggiornato raramente.

Adatto per: sistemi obsoleti, laboratori, test ambienti chiusi.

□□ Come testare il tuo browser

Vuoi sapere quanto è sicuro il tuo browser? Ecco tre test essenziali:

1. PrivacyTests.org

Analizza i browser in base a decine di metriche di privacy.

2. Cover Your Tracks (EFF)

Valuta fingerprint, blocco tracciatori e compatibilità con l'anonimato.

3. DNS Leak Test

Verifica se il tuo DNS espone la tua identità reale, anche con VPN attiva.

⚙ Bonus: impostazioni consigliate

Per aumentare la sicurezza del browser che già usi:

• Disattiva WebRTC
• Usa estensioni come uBlock Origin, Privacy Badger, HTTPS Everywhere
• Naviga in modalità incognito per ricerche OSINT mirate
• Imposta DNS su Cloudflare o NextDNS
• Blocca il fingerprint con CanvasBlocker

□□ Browser sicuro = indagine OSINT sicura

Chi lavora con **fonti aperte** e fa ricerca OSINT dovrebbe usare **Tor o LibreWolf**, impostando un profilo browser **dedicato all'indagine** per evitare contaminazioni con l'uso personale.

□□*Mai usare lo stesso browser per OSINT e social network personali.*

□□ Le false promesse della navigazione "anonima"

□□ Finestra in incognito: utile ma non sufficiente

Quando apri una **finestra in incognito** su Chrome, Brave o Firefox, ti senti più sicuro. Ma è davvero così?

La risposta è: **ni**.

Queste modalità, spesso chiamate "private" o "anonime", **non nascondono la tua identità al provider internet o ai siti che visiti**. Chi gestisce il server web sa **esattamente da dove vieni, cosa cerchi e che tipo di dispositivo usi**.

Quindi, a cosa servono?

□ **Eliminano automaticamente la cronologia di navigazione e i cookie al termine della sessione.**
□ **Impediscono ad altri siti, successivamente, di usare quei cookie per tracciarti.**

□□*Sono utili per evitare che altri utenti del tuo computer vedano la tua attività, non per proteggerti dal tracciamento esterno.*

□□ Il nemico invisibile: il fingerprinting

Oltre a cookie e tracciatori, c'è una tecnica ancora più subdola e invisibile: il **browser fingerprinting**.

Questa tecnica raccoglie **dati unici sul tuo browser e dispositivo** per costruire un profilo che ti identifica online anche **senza login o cookie**.

□□ Cosa raccoglie il fingerprinting?

• Risoluzione dello schermo
• Font installati
• Fuso orario
• Sistema operativo
• Plugin attivi
• Lingua del browser
• Versione JavaScript supportata
• …e molto altro.

□□ Quando queste informazioni vengono combinate, il risultato è una **"impronta digitale"** unica.

Anche se non conoscono il tuo nome, **sanno che sei “tu”**.

⚠ A chi serve?

• □□□□ Agli inserzionisti: per proporti pubblicità personalizzate
• □□♂ Alle piattaforme di analytics: per tracciare comportamenti
• □□□□ Anche a chi ha intenzioni meno legittime

□□ Come difendersi dal fingerprinting?

• Usa browser come LibreWolf o Tor, che limitano l’entropia delle informazioni trasmesse.
• Installa estensioni come CanvasBlocker, Trace o NoScript.
• Disattiva WebGL, WebRTC e i font personalizzati (se non ti servono).
• Modifica l'user agent del browser con strumenti come User-Agent Switcher.

□□ Ricorda: nessun sistema è perfetto. Ma **ridurre il livello di dettaglio trasmesso** è già un grande passo per la tua privacy.

□□ Vuoi approfondire?

• Prova LibreWolf per una privacy totale.
• Scarica Brave per una protezione immediata.
• Avvia le tue indagini su Tor Browser in totale anonimato.

□□ Hai dubbi o vuoi condividere le tue impostazioni ideali? Scrivici su Telegram o unisciti alla nostra newsletter!

I browser più sicuri del 2025

- **Combatti tracker e phishing,** quale il browser che scegii è strategico per bloccare tracciamenti invisibili è phishingg mirato.
- Ab**biamo testato** i 8 browser più sicuri del 2025: vediamo qual è il migllore per te.

Tabella comparativa

Browser	Blocco traccianti	VPN	Open Source
Brave	✓	✓	✓
LibreWolf	✓	✓	✓
Tor Browser	✓	✓	✓
Vivaldi	✓	✓	✗
Opera	✓	✗	✗

Testati: pro e contro

+ Blocco nativo tracker e ads

– Non completamente anonimo

+ Privacy estrema, no telemetria

– Navigazione anonima via rete Tor

– Vinií Proton e funzionalità avanzate

+ Facile da usare, siubarsocial

– VPN limitata e chiusa

Come difendertidi più

- Web in incognito non significa web anonimo! Usa Tor o LibréWolf per più protezione
- Installa estensioni anti-tracker come uBlock Origin
- Disabilita WebRTC per evitare “DNS leak”

→ **Guida completa su:**

coondivido.it/browser-sicuri-2025