Best Desktop Web Browsers for Privacy

Browser	Privacy Protections		Anonymity Potential		Fingerprinting Resistance		Cyber & Exploit Resilience		Usability Score	Extensions & Customization	Dev Team Trust	Tot
Brave	5	Blocks ads, trackers, fingerprints by default. Minimal telemetry.	4	No account needed. Tor integration. But defaults to Chromium-based infra.	4	Strong anti-fingerprint. Customization can create unique fingerprint.	5	5	Defaults are strong, requires minimal setup.	5	4	32
Brave + Extentions	5		4		4		5	4	Some breakage but still manageable.	5	4	31
Mullvad	5	Designed for anonymity. No user data. Integrates w/ Mullvad VPN.	5	No accounts. Mimics Tor's anon. while using VPN instead of Tor network.	5	Strong fingerprint defense. All users appear identical, cuts trackability.	5	4	Simple to use with strong defaults.	3	5	32
Mullvad + Extentions	5		5		5		5	3	More breakage with NoScript and fingerprinting blockers.	3	5	31
LibreWolf	5	Hardened Firefox fork w/ telemetry removed, privacy maxed.	4	No account req. Hardened security settings. Better than Firefox.	5	Tor-like fingerprinting protections, users blend together.	5	3	Harder to configure, privacy defaults cause some site issues.	4	5	31
LibreWolf + Extentions	5		5		5		5	2	NoScript especially makes it frustrating for beginners.	4	5	31
Tor	5	All traffic >> Tor network, blocking trackers, isolating web data.	5	Best for anonymity, hides IP, obscures traffic origins.	5	Makes users appear identical, removing fingerprinting risks.	5	2	Breaks many sites due to Tor network behavior.	2	5	29
Tor + Extentions	5		5		5		5	1	Too much breakage, requires expert knowledge.	2	5	28
DuckDuckGo	4	Blocks most tracking. Some dependencies on WebKit, Apple services.	3	Doesn't track, but lacks Tor/VPN integration. Mainstream infrastructure.	3	Basic fingerprinting protection but not as robust as Brave or Tor.	4	5	Works like a normal browser with privacy improvements.	3	4	26
DDG + Extentions	5		4		4		4	4	Some settings need adjusting, but still easy.	3	4	28
Firefox	3	Good tracking prevent, new TOS concerning >> potential data collection.	3	Account not required. But IP exposure, lack of Tor/VPN weaken anonymity.	3	Enhanced tracking prot. Default settings allow fingerprint leakage.	4	5	Familiar UI, needs some manual tweaks.	5	2	25
Firefox + Extentions	5		4		5		4	4	W/ NoScript, fingerprinting blockers, usability drops.	5	2	29
Safari	3	Intelligent Tracking Prevention (ITP), but Apple collects data.	2	No VPN, Tor. Apple accounts link browsing.	2	Some built-in protections, but Safari leaks unique identifiers	4	5	Extremely smooth. Best for Apple users if usability > extreme privacy.	2	3	21
Safari + Extentions	4		2		3		4	4	Some extensions break functionality.	3	3	23
Opera	2	Built-in ad blocker. History of ??? privacy practices. China-linked.	2	Free VPN, but logs usage, has weak security.	2	Weak fingerprinting protection, leaving users exposed to tracking.	3	5	No major usability hurdles.	3	2	19
Opera + Extentions	3		3		2		3	4	Some breakage with aggressive settings.	3	2	20
Chrome	1	Google's data collection hub. Tracks browsing. Ties user accounts.	1	Tightly linked to Google services, requiring sign-in for full functionality.	1	Actively fingerprintings you, making tracking easy for advertisers.	4	5	Extremely user-friendly (but not private).	5	1	18
Chrome + Extentions	2		2		1		4	5	Improves privacy, doesn't hurt usability	5	1	20
Edge	1	Microsoft telemetry, tracking everything: browsing to keystrokes.	1	Tied to Microsoft accounts, with zero focus on anonymous browsing.	1	No fingerprinting defenses, making users easy to track.	3	5	Very user-friendly, deeply integrated with Windows.	4	1	16
Edge + Extentions	2		2		1		3	5	Extensions don't cause major usability issues.	4	1	18

Privacy Protections: Measures built-in tracking, ad, and fingerprinting blockers. Higher scores mean stronger privacy defaults.
Anonymity Potential: Evaluates how well the browser hides user identity (e.g., Tor, VPN, account requirements).
***Fingerprinting* Resistance**: Assesses how easily a browser can be uniquely identified by websites. Higher scores mean less trackability.
Cyber & Exploit Resilience: Rates security features against exploits, malware, and data breaches.
Usability Score: Balances privacy with ease of use; higher scores mean fewer site breakages and a smoother experience.
Extensions & Customization: Measures how well a browser supports privacy extensions and manual security tweaks.
Dev Team Trust: Evaluates the browser developer's reputation, history, and commitment to user privacy. Higher scores mean a more trustworthy team.

Privacy-Focused Users / Corporate
(Everyday Users Who Want Strong Privacy Without Too Much Breakage)

Best Choice: **Brave**

Blocks ads, trackers, and fingerprints by default. Has Tor integration for extra anonymity if needed. High usability with minimal setup required.

Alternative: LibreWolf
Safari (for macOS-Only Users in Corporate environments)

High-Security & Anonymity Users
(Journalists, Activists, Whistleblowers, High-Risk Individuals)

Best Choice: **Tor**

Highest anonymity with traffic routed through the Tor network. Strongest fingerprinting resistance (all users appear identical). Downsides: Breaks many websites, slow performance, requires expertise.

Alternative: Mullvad

Casual Users Who Want Some Privacy
(Mainstream Users Who Want Better Defaults W/O Losing Convenience)

Best Choice: **DuckDuckGo**

Blocks most trackers and offers a familiar browsing experience. No extreme breakage like Tor or LibreWolf. Not as strong on fingerprinting protection as Brave or Mullvad.

Alternative: Safari (on Apple Devices Only)
Firefox (With Extensions)

'+ Extentions' option use of these if available for the browser: *UBlock*, *PrivacyBadger*, *Decentraleyes*, *NoScript, CanvasBlocker, User-Agent Switcher, Clear URLs*.

*Browser features change often. This affects scoring.

Best Mobile Web Browsers for Privacy

Browser		Privacy Protections	Anonymity Potential	Fingerprinting Resistance	Cyber & Exploit Resilience	Usability Score	Extensions & Customization	Dev Team Trust	Tot
Brave	iOS	4	3	2	4	5	1	4	23
	Android	4	3	3	4	5	2	4	25
Mullvad	iOS	5	5	3	5	4	1	5	28
	Android	5	5	4	5	4	2	5	30
LibreWolf	iOS	4	3	2	4	3	1	5	22
	Android	4	4	3	4	3	2	5	25
Tor	iOS	5	5	4	4	2	1	5	26
	Android	5	5	5	4	2	1	5	27
DuckDuckGo	iOS	3	3	2	3	5	1	4	21
	Android	3	3	2	3	5	2	4	22
Safari	iOS	3	2	2	4	5	2	3	21
Firefox	iOS	3	3	2	3	5	2	2	20
	Android	4	3	3	3	5	3	2	23
Opera	iOS	2	2	1	2	5	1	2	15
	Android	3	2	1	2	5	2	2	17
Chrome	iOS	1	1	1	3	5	1	1	13
	Android	2	2	1	3	5	2	1	16
Edge	iOS	1	1	1	2	5	1	1	12
	Android	2	1	1	2	5	2	1	14

Privacy Protections: Measures built-in tracking, ad, and fingerprinting blockers. Higher scores mean stronger privacy defaults.
Anonymity Potential: Evaluates how well the browser hides user identity (e.g., Tor, VPN, account requirements).
***Fingerprinting* Resistance**: Assesses how easily a browser can be uniquely identified by websites. Higher scores mean less trackability.
Cyber & Exploit Resilience: Rates security features against exploits, malware, and data breaches.
Usability Score: Balances privacy with ease of use; higher scores mean fewer site breakages and a smoother experience.
Extensions & Customization: Measures how well a browser supports privacy extensions and manual security tweaks.
Dev Team Trust: Evaluates the browser developer's reputation, history, and commitment to user privacy. Higher scores mean a more trustworthy team.

Best Privacy Browsers for iOS (2025)

Use Case	Top	Why for iOS
Overall Privacy	**Mullvad**	No telemetry, strong fingerprint resistance, based on hardened Firefox.
Anonymity	Tor	Routes traffic through Tor, hides IP, strongest anon. but breaks many sites.
Privacy + Usability	**Brave**	Blocks ads & trackers by default, good usability, suffers from WebKit limits.
Casual Privacy	Safari	(w/ extentions) Best balance of privacy + usability for Apple users.
Advanced Users	LibreWolf	Hardened Firefox, no telemetry, fingerprinting resist, some usability issues.
Mainstream Compat.	Safari	(w/ extentions) More private than Firefox due to WebKit sandboxing.

Best Privacy Browsers for Andriod (2025)

Use Case	Top	Why for Android
Overall Privacy	**Mullvad**	Fully private, no telemetry, strongest fingerprinting resistance.
Anonymity	Tor	Uses the Tor network, hides IP, strongest anonymity but very slow.
Privacy + Usability	**Brave**	Blocks ads & trackers by default, better extension support than iOS.
Casual Privacy	DDG	Simple, good tracker blocking, but weaker fingerprint resistance.
Advanced Users	LibreWolf	Hardened Firefox fork with no telemetry, strong fingerprinting protection.
Mainstream Compat.	Firefox	Gecko (not WebKit), decent tracking prevent, best for compatibility.

Privacy Extention options for Android: *UBlock*, *PrivacyBadger*, *Decentraleyes*, *NoScript, CanvasBlocker, User-Agent Switcher, Clear URLs.*
Privacy Extention options for iOS: *1Blocker*, *User-Agent Switcher, StopTheMadness, Privacy Redirect*

*Browser features change often. This affects scoring.