Premessa

Proteggere la propria privacy online non è solo una questione di sicurezza personale, ma anche un atto di consapevolezza e autodeterminazione.
Ogni clic, ogni ricerca, ogni connessione a Internet lascia una traccia indelebile.
Navigare con un browser sicuro e ben configurato è un primo passo verso un uso più consapevole della rete. Anche la libertà è una disciplina che va allenata.

Va tenuto presente che queste configurazioni potrebbero limitare l'accesso a determinati siti o servizi. Ma questa limitazione è anche una rivelazione: quali siti sono davvero indispensabili?

Il consenso è reale solo se informato. Questa guida ti aiuterà a prendere decisioni più consapevoli sulla tua presenza online.

1] Aprire Firefox
2] Nella barra di ricerca digitare: about:config
3] Firefox ti avviserà di "Procedere con cautela" >> consapevole che, chi è pronto a cedere la propria libertà per un po' di sicurezza non merita né l'una né l'altra, "Accetta il rischio e continua"
4] Nella barra di ricerca delle preferenze iniziamo a cercare e modificare SOLO i valori riportati di seguito.

*Se hai dubbi rispetto i punti elencati di seguito non andare oltre il punto 4.

---

1. Disabilitare WebRTC
WebRTC può rivelare il tuo indirizzo IP reale anche con una VPN o Tor.
In Firefox, vai su: about:config e imposta:
- media.peerconnection.enabled = false

2. Bloccare il Fingerprinting
Firefox può resistere al fingerprinting avanzato impostando:
- privacy.resistFingerprinting = true
- privacy.trackingprotection.fingerprinting.enabled = true

3. Disabilitare il Tracking e i Cookie di Terze Parti
Blocca pubblicità invasive e tracking cross-site:
- privacy.trackingprotection.enabled = true
- privacy.trackingprotection.cryptomining.enabled = true
- privacy.trackingprotection.socialtracking.enabled = true
- network.http.referer.XOriginPolicy = 2
- network.http.referer.XOriginTrimmingPolicy = 2

4. Disabilitare Telemetria e Raccolta Dati
Firefox raccoglie dati per migliorare l'esperienza utente.
Disabilita tutte le impostazioni di telemetria per maggiore privacy:
- toolkit.telemetry.enabled = false
- toolkit.telemetry.archive.enabled = false
- toolkit.telemetry.server = ''
- datareporting.healthreport.uploadEnabled = false
- browser.send_pings = false

[ATTENZIONE] Prima di modificare i DNS e Tor:
Usare DNS di Cloudflare o navigare tramite Tor potrebbe causare problemi o rallentamenti del traffico:
- Cloudflare potrebbe registrare dati di navigazione, nonostante sia considerato più sicuro di altri provider.
- Usare Tor direttamente su Firefox potrebbe non offrire lo stesso livello di anonimato del Tor Browser, perché alcune configurazioni potrebbero raccogliere dati di navigazione.

---

5. Usare DNS Sicuri e Disabilitare DoH
Se vuoi usare DNS cifrati, usa Cloudflare (1.1.1.1) o Quad9 (9.9.9.9):
- network.trr.mode = 3
- network.trr.uri = 'https://mozilla.cloudflare-dns.com/dns-query'
- network.trr.bootstrapAddress = '1.1.1.1'
Se invece vuoi usare una VPN con DNS personalizzati, disabilita DoH:
- network.trr.mode = 5

6. Configurare Firefox per Usare Tor
Per navigare in modo anonimo con Tor senza usare il Tor Browser, configura Firefox così:
- network.proxy.socks = 127.0.0.1
- network.proxy.socks_port = 9050
- network.proxy.socks_version = 5
- network.proxy.type = 1
- network.proxy.socks_remote_dns = true
Avvia Tor con il comando:
sudo systemctl start tor

[ATTENZIONE] Sulle estensioni per la privacy:
L'uso di estensioni può esporre a rischi di data leak, poiché alcune estensioni potrebbero comunque raccogliere dati di navigazione.
Per ridurre il rischio, installa solo estensioni open-source e con buona reputazione.

---

7. Installare Estensioni per la Privacy (Opzionale)
Se decidi di installarle, ecco alcune consigliate:
- uBlock Origin
- NoScript
- Privacy Badger
- Decentraleyes
- CanvasBlocker
