# Firefox Saugios Konfigūracijos Gidas

**Autorius:** Deividas Ambrazevičius | **Data:** Jun 2, 2026

## Įvadas

Šiame gide rasite patarimus, kako saugiai sukonfigūruoti savo interneto naršykles. Kasdieniam naudojimui rekomenduojama rinktis „Firefox“ (kompiuteriams).

**Kodėl „Firefox“?** Skirtingai nei komercinės naršyklės, „Firefox“ priklauso ne pelno siekiančiai organizacijai, kurios pagrindinis tikslas - jūsų privatumas, o ne duomenų pardavimas. Ši naršyklė automatiškai blokuoja paslėptus sekiklius ir stipriai izoliuoja kiekvienos svetainės slapukus, neleisdama trečiosioms šalims rinkti jūsų naršymo istorijos.

**Konteineriai naršymo atskyrimui** yra unikali „Firefox“ funkcija, kuri leidžia suskirstyti naršymą į visiškai izoliuotus „konteinerius“ (pvz., Darbas, Asmeninis, Bankai). Tai reiškia, kad viename skirtuke atidaryti socialiniai tinklai negali jūsų sekti, kai kituose skirtukuose naršote naujienas ar apsiperkate.

> **DETALIAU:** Jei norite skaityti detalius paaiškinimus, ką reiškia kiekviena funkcija, tikslius nustatymų žingsnius ir konfigūracijas rasite gido pabaigoje.

## Naršyklės įdiegimas ir pagrindiniai nustatymai

Rekomenduojama naudoti tik „Firefox“ interneto naršyklę visoms internetinėms užduotims. „macOS“ vartotojai ją gali įsidiegti per terminalą naudodami šią komandą (jei naudoja Homebrew):

```
brew install --cask firefox
```

Įdiegus „Firefox“, atlikite šiuos pakeitimus (jie labai panašūs tiek „Linux“, tiek „macOS“ ar „Windows“ sistemose). Spustelėkite „Firefox“ meniu viršutiniame dešiniajame kampe ir pasirinkite **„Settings“** arba **„Preferences“**.

### Skiltis „General“

- Atžymėkite "Recommend extensions as you browse".
- Atžymėkite "Recommend features as you browse".

### Skiltis "Home"

- Pakeiskite "Homepage and new windows" ir "New tabs" į "Blank page".
- Išjunkite visas "Firefox Home Content" parinktis.

### Skiltis "Search"

- Atžymėkite visas parinktis po "Provide search suggestions".

## Skiltis "Privacy & Security"

- Išvalykite (atžymėkite) viską "Address Bar" meniu.
- Pasirinkite "Strict" apsaugą.
- Pažymėkite "Tell websites not to sell or share my data" ir "Do Not Track".
- Pažymėkite "Delete cookies and site data when Firefox is closed".

- Atžymėkite "Show alerts about passwords for breached websites".
- Atžymėkite "Suggest Firefox Relay...".
- Atžymėkite "Suggest strong passwords".
- Atžymėkite "Fill usernames and passwords".
- Atžymėkite "Ask to save passwords".
- Atžymėkite "Save and fill addresses".
- Pažymėkite „Max Protection“ Enable DNS over HTTPS using.
- Atžymėkite "Save and fill payment methods".
- Pakeiskite "History" nustatymą į "Firefox will use custom settings for history".
- Atžymėkite "Remember browsing and download history" ir "Remember search and form history".
- Pažymėkite "Clear history when Firefox closes".

> **Dėmesio:** Nepažymėkite "Always use private browsing mode", nes tai sugadins "Firefox Containers" funkciją.

- Skiltyje "Permissions", paspauskite "Settings" šalia Location, Camera, Notifications ir Virtual Reality. Kiekviename iš jų pažymėkite langelį "Block new requests...". (Tą patį atlikite su "Microphone", jei neskambinsite per naršyklę).
- Atžymėkite visas parinktis po "Firefox Data Collection and Use".
- Atžymėkite visas parinktis po "Website Advertising Preferences".
- Atžymėkite visas parinktis po "Deceptive Content and Dangerous Software Protection".
- Pažymėkite "Enable HTTPS-Only Mode in all windows".

> **Svarbi pastaba apie about:config:** Anksčiau buvo rekomenduojama keisti gilius naršyklės nustatymus per about:config, tačiau dabar to daryti nerekomenduojama. Bandymai pernelyg paslėpti savo tapatybę keičiant specifinius nustatymus paverčia jūsų naršyklę per daug unikalia (browser fingerprinting) ir leidžia jus sekti dar lengviau, nes išsiskiriate iš minios.
>
> **about:config pakeitimai (su išlygomis):** Suraskite nustatymą `privacy.resistFingerprinting` ir nustatykite į **true**. Tai padeda sumažinti naršyklės atpažinimą pagal "pirštų atspaudus".

## Numatytasis paieškos variklis (Default Search Engine)

Nors "DuckDuckGo" privatumo politika yra geresnė nei "Google", rekomenduojama apsvarstyti SearXNG naudojimą. Tai yra atvirojo kodo metapaieškos variklis, kuris agreguoja rezultatus iš "Google", "Bing" ir kitų, bet nesidalina vartotojų informacija su šiais varikliais.

### Kaip nustatyti SearXNG "Firefox" naršyklėje:

1. Apsilankykite viešame serveryje (pvz., `https://searx.space/`) ir atlikite bet kokią paiešką.
2. Dešiniuoju pelės mygtuku spustelėkite ant adreso (URL) juostos ir pasirinkite "Add" šalia padidinamojo stiklo piktogramos.
3. Eikite į "Firefox" "Settings" meniu ir spustelėkite "Search".
4. Pakeiskite "Default search engine" į naujai pridėtą parinktį.

### Jei norite išsaugoti SearXNG nustatymus (pvz., tamsiąją temą) be išsitrynimo:

1. Eikite į "Firefox" "Settings" -> "Privacy & Security".
2. Spustelėkite "Manage Exceptions" šalia "Delete cookies...".
3. Įveskite pasirinkto SearXNG serverio adresą (pvz., `https://searx.work`).
4. Spustelėkite "Allow" ir "Save Changes".

## Naudingi naršyklės plėtiniai (Add-ons)

### A) uBlock Origin

Tai svarbiausias plėtinys, kuris blokuoja reklamas, sekimo skriptus ir kenkėjišką kodą.

- **Įdiegimas:** Eikite į `addons.mozilla.org/en-US/firefox/addon/ublock-origin/`. Spustelėkite "Add to Firefox". Patvirtinkite leisti veikti privačiame režime ("Allow the extension to run in private mode").
- **Išplėstiniai nustatymai:** Paspauskite "uBlock Origin" piktogramą meniu ir pasirinkite "Dashboard".
  - Kortelėje "Settings", pažymėkite "I am an advanced user".
  - Kortelėje "Filter List" įjunkite papildomus rinkinius: po "Privacy" pažymėkite "Block Outsider Intrusion into LAN", o po "Annoyances" pažymėkite visą "EasyList" sekciją. Spustelėkite "Update Now".

### B) Multi-Account Containers

Tai oficialus "Mozilla" plėtinys, leidžiantis atskirti skirtingus naršymo seansus. Kiekvienas konteineris turi savo atskirą slapukų (cookies) ir vietinės saugyklos aplinką.

#### Kodėl tai naudinga?

- **Apsauga nuo sekimo (Anti-Tracking):** Socialiniai tinklai (pvz., "Facebook" ar "Google") negali jūsų sekti kitose svetainėse, jei juos atidarote tik jiems skirtame konteinerio.
- **Kelių paskyrų valdymas vienu metu:** Galite naudotis dviem skirtingomis "Gmail" ar "Twitter" paskyromis skirtinguose konteineriuose tame pačiame lange.
- **Saugumas nuo duomenų nutekėjimo (Session Hijacking):** Kenkėjiška svetainė viename konteineryje negalės pavogti prisijungimo sesijų iš kitų konteinerių.

**Kaip naudotis?** Įdiekite plėtinį iš `addons.mozilla.org`. Spustelėkite plėtinio piktogramą (tris kvadratėlius) viršuje dešinėje. Norėdami sukurti/redaguoti, paspauskite "Edit Containers" arba "+". Atsidarykite svetainę, paspauskite plėtinio piktogramą ir pažymėkite langelį šalia "Always open in... [Konteinerio Pavadinimas]".

> **PRAKTINIS PATARIMAS:** Nors "Firefox" funkcija "Total Cookie Protection" puikiai izoliuoja slapukus, konteineriai vis tiek suteikia papildomą apsaugą. Rekomenduojama susikurti atskirus konteinerius savo el. paštui, socialiniams tinklams ir bankams.

## Kaip pasikeis jūsų naršymo patirtis

Pritaikius visus šiuos griežtus "Firefox" nustatymus, jūsų kasdienis naršymas internete taps gerokai saugesnis, tačiau prie kai kurių pokyčių reikės priprasti. Didžiausias skirtumas slypi balanse tarp privatumo ir patogumo.

| Įprastas naršymas | Griežtai sukonfigūruotas "Firefox" naršymas |
|---|---|
| Svetainės prisimena jus visą laiką. | Kiekvieną kartą atidarius naršyklę, teks prisijungti iš naujo (nebent padarysite išimtis). |
| Gausu personalizuotų reklamų ir pasiūlymų. | Jokių reklamų, iššokančių langų ar sekimo skriptų (dėka "uBlock Origin"). |
| Vasi slapukai ir istorija saugomi vietoje. | Uždarius naršyklę, ištrinama visa istorija, nepaliekant pėdsakų kompiuteryje. |
| Paieškos rezultatai pritaikyti pagal jūsų profilį. | "SearXNG" pateikia neutralius, nepersonalizuotus ir objektyvesnius rezultatus. |
| Visos svetainės atidaromos vienoje erdvėje. | Skirtingos paskyros ir svetainės griežtai atskirtos konteineriuose. |
| Svetainės visada veikia sklandžiai. | Kartais per griežtas blokavimas gali iškraipyti svetainės išvaizdą ar funkcijas. |

### Kaip bus apsaugomi jūsų duomenys

- **Konteinerių izoliacija:** "Multi-Account Containers" užtikrina, kad tokios platformos kaip "Facebook" ar "Google" negalės matyti, kokiose kitose svetainėse lankotės.
- **Nulinis vietinis pėdsakas:** Kadangi naršyklė neįsimena formų, slaptažodžių ir ištrina slapukus po uždarymo, net ir fizinę prieigą prie jūsų kompiuterio gavęs asmuo nematys jūsų naršymo istorijos.
- **Apsauga nuo profiliavimo ("Fingerprinting"):** Pakeitus `privacy.resistFingerprinting` nustatymą, jūsų naršyklė svetainėms atrodys lygiai taip pat, kaip tūkstančiai kitų.
- **Paslėptos užklausos:** "DNS over HTTPS" šifruoja jūsų srautą, todėl jūsų interneto paslaugų teikėjas (ISP) negali matyti, kokius tinklalapius bandote atidaryti.
- **Trečiųjų šalių blokavimas:** "uBlock Origin" ir griežtas "Firefox" režimas automatiškai atmeta užklausas į žinomus duomenų rinkėjų serverius.

## PABAIGAI

Šis perėjimas reiškia jūsų mąstysenos pokytį - nuo pasyvai interneto vartotojo, kurio asmeniniai duomenys yra parduodama prekė, pereinate prie aktyvaus savo skaitmeninės erdvės šeimininko.

Iš pradžių šis naujas naršymo būdas gali atrodyti nepatogus. Jums reikės išorinės slaptažodžių tvarkyklės, nes naršyklė jūsų slaptažodžių nebeprisimins. Turėsite sąmoningai galvoti, kurį "konteinerį" atidaryti konkrečiai užduočiai (pvz., el. bankininkystei), o retkarčiais teks išjungti "uBlock Origin" apsaugą, kad per daug užblokuota svetainė vėl suveiktų.

Tačiau šis nedidelis patogumo praradimas yra kaina už ramybę ir skaitmeninę higieną. Jūsų paieškos įpročiai, ligų simptomų paieškos, politinės pažiūros ir pomėgiai nustos pildyti didžiųjų korporacijų duomenų bazes. Jūs matysite greitesnį, švaresnį internetą be manipuliuojančių reklamų, o jūsų skaitmeninis identitetas bus valdomas tik jūsų pačių. Tai ilgalaikė investicija į jūsų privatumą, kuri greitai taps natūraliu, kasdieniu įpročiu.

## Išsamus nustatymų reikšmės paaiškinimas

Čia detaliai paaiškinama, kodėl atlikome aukščiau nurodytus pakeitimus ir kaip jie prisideda prie jūsų saugumo bei privatumo internete.

### Skiltis "General“ (Bendrieji nustatymai)

- **Atžymėti "Recommend extensions...":** Neleidžia jūsų interneto naršymo informacijos siųsti į "Firefox" serverius analizėms. Tai apsaugo jūsų naršymo įpročių privatumą nuo pačios naršyklės kūrėjų.

### Skiltis "Home“ (Pradžios langas)

- **Pakeisti "Homepage..." į "Blank page":** Neleidžia automatiškai įkelti numatytojo puslapio atidarant naršyklę. Taip išvengiama nereikalingų foninių ryšių ir duomenų atsisiuntimo iš "Mozilla" serverių.
- **Išjungti "Firefox Home Content":** Pašalina naujienų ir rėmėjų nuorodas naujame skirtuke. Tai apsaugo nuo trečiųjų šalių turinio teikėjų, kurie galėtų registruoti jūsų parodymus ar paspaudimus.

### Skiltis "Search“ (Paieška)

- **Atžymėti paieškos siūlymus:** Neleidžia vedamų užklausų siųsti tiesiai į "Google" (ar kitą variklį) dar nespėjus paspausti "Enter". Taip apsaugoma nuo profiliavimo renkant nebaigtas ar atšauktas paieškos frazes.

### Skiltis "Privacy & Security“ (Privatumas ir saugumas)

- **Išvalyti viską "Address Bar" meniu:** Neleidžia adreso juostoje siūlyti anksčiau lankytų svetainių ar žymų – fizinio privatumo apsauga.
- **Pasirinkti "Strict" apsaugą:** Blokuoja žinomus sekiklius, kriptovaliutų kasėjus ir tarp-svetaininius slapukus.
- **Pažymėti "Do Not Track":** Aktyvus privatumo teisių išreiškimas prašant atidarytų svetainių jūsų nesekti ir neparduoti duomenų.
- **Pažymėti "Delete cookies... when Firefox is closed":** Uždarius naršyklę ištrinami svetainių failai ir sesijos. Apsaugo nuo ilgalaikio sekimo.
- **Atžymėti įspėjimus apie nutekėjusius slaptažodžius:** Apriboja naršyklės komunikaciją su trečiųjų šalių serveriais, išjungiant užklausas į išorines duomenų bazes.
- **Atžymėti slaptažodžių saugojimą ir siūlymą:** Apsaugos tikslais naršyklės nėra saugiausia vieta laikyti slaptažodžius. Tam naudokite atskiras, šifruotas tvarkykles.
- **Atžymėti "Save and fill addresses/payment methods":** Apsaugo jautrius duomenis vagystės atveju, jei kas nors gautų fizinę prieigą prie kompiuterio.
- **Pritaikyti istorijos nustatymai (Clear history...):** Garantuoja, kad po jūsų sesijos neliks jokios istorijos (neprarandant konteinerių funkcijos).
- **"Block new requests..." (Kamerai, mikrofonui):** Blokuoja iššokančius svetainių langus prašančius prieigos. Apsaugo nuo netyčinio stebėjimo.
- **Atžymėti "Firefox Data Collection...":** Visiškai sustabdo telemetrijos siuntimą "Mozilla“ kompanijai.
- **Atžymėti "Deceptive Content... Protection":** Apsaugo nuo naršymo istorijos dalinimosi, nes norint apsaugoti nuo virusų, naršyklė turi siųsti jūsų lankomų svetainių adresus trečiosioms šalims patikrai.
- **Pažymėti "Enable HTTPS-Only Mode":** Priverstinai naudoja tik šifruotą HTTPS ryšį, apsaugant duomenis nuo perėmimo.

### privacy.resistFingerprinting (Nustatyta į true)

**Ką tai daro:** Šis nustatymas įjungia apsaugą nuo vadinamojo naršyklės pirštų atspaudų rinkimo. Užuot sekę jus per slapukus (cookies), reklamuotojai ir sekimo sistemos surenka unikalią informaciją apie jūsų įrenginį: ekrano raišką, operacinę sistemą, įdiegtus šriftus, laiko juostą, kalbą ir kt. Įjungus šį nustatymą, Firefox pradeda klastoti šią informaciją, bandydama priversti jūsų naršyklę atrodyti visiškai standartiškai ir identiškai tūkstančiams kitų vartotojų (tai technologija, pasiskolinta iš Tor naršyklės).

### Saugus DNS ir "DNS over HTTPS“ (DoH)

**Ką tai daro:** Standartiškai šios užklausos yra nešifruotos, o tai reiškia, kad jūsų interneto tiekėjas (Telia, Bite, Tele2 ir pan.) tiksliai mato, kokias svetaines lankote, net jei pati svetainė yra saugi (HTTPS). Įjungus DoH (DNS over HTTPS), jūsų DNS užklausos yra užšifruojamos ir paslepiamos nuo interneto tiekėjo. Pasirinkus Cloudflare (1.1.1.1) orientuojamasi į greitį ir privatumą, o Quad9 (9.9.9.9) papildomai blokuoja žinomas kenkėjiškas svetaines.

**Išlygos ir galimos problemos:** „Maximal protection“ rizika: Firefox nustatymuose parinkus maksimalią apsaugą, naršyklė niekada nenaudos nešifruoto DNS. Jei jūsų pasirinktas saugus DNS serveris (pvz., Cloudflare) laikinai sutriks, arba jei viešbučio/kavinės Wi-Fi blokuos DoH, jūsų visiškai neteksite interneto ryšio naršyklėje, kol nepakeisite nustatymų.

### „Decentraleyes“ plėtinys

**Ką tai daro:** Daugelis svetainių naudoja tuos pačius išteklius (šriftus, programinio kodo bibliotekas), kuriuos užkrauna iš didžiųjų serverių (CDN), pavyzdžiui, Google ar Cloudflare. Tai reiškia, kad net jei blokuojate Google sekiklius, Google vis tiek mato jūsų IP adresą, kai svetainė prašo atsiųsti reikalingą šriftą. Decentraleyes laiko šių populiarių išteklių kopijas jūsų kompiuteryje. Kai svetainė prašo failo iš Google, plėtinys jį blokuoja ir akimirksniu paduoda failą iš jūsų kompiuterio atminties.

**Išlygos ir galimos problemos:** Mažėjanti nauda: Nors idėja puiki, modernios naršyklės (ypač Firefox) įdiegė technologiją, vadinamą Network Partitioning (arba Total Cookie Protection), kuri labai apriboja CDN galimybes jus sekti per skirtingas svetaines. Pasenę failai: Decentraleyes atnaujinamas gana retai. Kartais svetainėms reikia pačios naujausios kodo versijos, o plėtinys paduoda seną. Dėl to kai kurios svetainės gali veikti su klaidomis. (Daugelis entuziastų dabar naudoja alternatyvą, vadinamą LocalCDN, nes ji atnaujinama dažniau).